

**Л<sub>A</sub>T<sub>E</sub>X Blockchain технологийг  
сонгуулийн санал хураалтад ашиглах нь**

Горилогч

© Э.Төгөлдөр

Энэхүү бүтээл нь

*"Системийн аюулгүй байдал"* -аар баклаврын зэрэг

горилсон бүтээлд тавигдах

шаардлагыг бүрэн хангасан болно

*Мэдээллийн сүлжээ аюулгүй байдал*

Шинжлэх Ухаан Технологийн Их Сургууль

2017-10-18

Улаанбаатар хот

# Гарчиг

<b>Хүснэгтийн жагсаалт</b>	<b>v</b>
<b>Зургийн жагсаалт</b>	<b>vi</b>
<b>1 Удиртгал</b>	<b>1</b>
1.1 Зорилго . . . . .	1
1.2 Зорилт . . . . .	1
<b>2 Онол</b>	<b>3</b>
2.1 Блокчэйн технологи . . . . .	3
2.1.1 Түүх . . . . .	3
2.1.2 Блокчэйн гэж юу вэ . . . . .	6
2.1.3 Блокчэйн юу хийдэг вэ . . . . .	7
2.1.4 Блокчэйн яагаад хэрэгтэй вэ . . . . .	8
2.1.5 Блокчэйний бүтэц . . . . .	9
2.1.6 Блокийн гинж (чэйн) . . . . .	10
2.1.7 Replicated database . . . . .	11
2.1.8 Блокчэйний төрлүүд . . . . .	12
2.1.9 Блокчэйний хөгжлийн үе шат . . . . .	13
2.1.10 Тохиролцооны алгоритм . . . . .	14
2.1.11 Блокчэйн хэрэглээнд . . . . .	15
2.1.12 Өнөөгийн блокчэйний хэрэглээ . . . . .	16
2.1.13 Блокчэйн аппликэйшн ирээдүйд . . . . .	16
2.1.14 Блокчэйнийг хүрээлэн буй орчин . . . . .	17
2.1.15 Технологи болон хууль, эрх зүй . . . . .	17
2.1.16 Блокчэйний боломжууд . . . . .	18

2.2	Төвлөрсөн бус сүлжээ (Decentralized network)	18
2.2.1	Төвлөрсөн бус сүлжээний архитектур	21
2.2.1.1	Бүтэцлэгдээгүй сүлжээ	22
2.2.1.2	Бүтэцлэгдсэн сүлжээ	23
2.2.1.3	Хосолмол загвар	24
2.3	Нууцлал аюулгүй байдал	24
2.3.1	Хаш функц	24
2.3.2	Хаш функцийн төрлүүд	25
2.3.3	Өөрчлөлтийг илрүүлэх	25
2.3.4	Давхцал	25
2.3.5	Нэг чиглэлт функц	26
2.3.6	Шахалт	26
2.3.7	Хаш функц блокчэйн хэрхэн хэрэглэгддэг вэ	26
2.3.8	Нийтийн түлхүүртэй нууцлалын алгоритм	26
2.3.9	RSA алгоритм	27
2.3.10	Цахим гарын үсэг	29
2.4	Тохиролцооны протоколууд	32
2.4.1	PoW(Proof of Work)	32
2.4.2	Эцэслэн шийдэх чанар(finality)	35
2.4.3	Ухаалаг гэрээ(Smart contract)	37
<b>3</b>	<b>Судалгаа</b>	<b>39</b>
3.1	Блокчэйн технологи хэрхэн ажилладаг вэ	39
3.1.1	Криптограф түлхүүр	40
3.1.2	Тархсан сүлжээ	41
3.1.3	Бичилтийн систем	41
3.1.4	Протокол	42
3.1.5	Блок хэрхэн үүсдэг вэ	44
3.2	Блокийн багтаамж	45
3.2.1	Блок хэмжээний асуудал	46
3.2.2	Давуу тал	47
3.2.3	Сул тал	47



# Хүснэгтийн жагсаалт

# Зургийн жагсаалт

2.1	Блокчэйн сүлжээний бүтэц . . . . .	8
2.2	Блокийн гинж . . . . .	11
2.3	Блокчэйний ажиллагаа . . . . .	14
2.4	Криптовалиут арилжааны платформ . . . . .	15
2.5	P2P сүлжээ . . . . .	19
2.6	Unstructured . . . . .	22
2.7	Structured p2p . . . . .	23
2.8	MD5 хаш функ . . . . .	25
2.9	SHA256 . . . . .	25
2.10	Нийтийн түлхүүртэй алгоритм . . . . .	27
2.11	Цахим гарын үсэг . . . . .	31
2.12	Гүйлгээний мэдээллийг зассан үед . . . . .	34
3.1	Блокчэйн бүтэц . . . . .	39
3.2	Хэрэглэгчид . . . . .	40
3.3	Хувийн болон нийтийн түлхүүр . . . . .	40
3.4	Цахим гарын үсэг . . . . .	40
3.5	Бичилт . . . . .	41
3.6	Блок . . . . .	42
3.7	Протокол . . . . .	43
3.8	Блокын гинж . . . . .	43
3.9	Хаш хүснэгт . . . . .	44
3.10	Блокийн загвар . . . . .	45

# Бүлэг 1

## Удиртгал

### 1.1 Зорилго

Энэхүү төслийн ажлын зорилго нь блокчэйн технологийг судалсан судалгаан дээрээ тулгуурлан сонгууль болон санал хураалтын үйл ажиллагаанд энэ технологийг нэвтрүүлэн ашиглах боломжийг туршиж судлах юм.

### 1.2 Зорилт

Дээрх зорилгыг хэрэгжүүлэхийн тулд дараах зорилтыг мөрдөж ажиллаа :

- Блокчэйн технологийн үндэс
- Блокчэйн технологийн бүтэц үйл ажиллагаа
- Блокчэйн технологийн ашиглалт ба ирээдүйн боломжууд
- Блокчэйн технологи нийгэмд
- Төвлөрсөн бус сүлжээний бүтэц ангилал
- Нууцлал аюулгүй байдлын алгоритмууд
- Баталгаажуулалтын протоколууд
- Монгол улсад сонгуулийн үйл ажиллагаа хэрхэн явагддаг тухай
- Сонгуулийн тухай хуулиуд

- Блокчэйн технологи ашиглах давуу тал
- Бусад орнуудад энэ талаар хэрхэн судалж байгаа тухай
- Бусад хэрэгжсэн байгаа төслүүд
- Дээрх онол болон судалгааны мэдлэг дээр тулгуурлан Блокчэйн технологид суурилсан санал хураалтын програм хөгжүүлэн турших



## Бүлэг 2

## Онол

### 2.1 Блокчэйн технологи

#### 2.1.1 Түүх

Интернетийн хөгжлийн эхэн үед бид и-мэйл, World Wide Web, dot-com, нийгмийн сүлжээ, хөдөлгөөнт Веб, big data, үүлэн тооцоолол болон зүйлсийн интернет зэрэгтэй танилцсан. Энэ үе нь бидэнд хайлт, хамтран ажиллагаа болон мэдээлэл солилцооны зардлыг багасгахад маш их тус болсон. Түүнчлэн шинэ төрлийн медиа, байгууллагын зохион байгуулалт болон жижиглэн худалдааны шинэ хэв маягийг нэвтрүүлсэн. Мэдрэгч технологийг нэмснээр бидний түрийвч, хувцас, тээврийн хэрэгсэл, байшин барилга, хот, түүнчлэн бидний биологид хүртэл ухаалаг системийг ашиглах болсон.

Нэгтгэн дүгнэхэд сүүлийн хориодхон жилд Интернет өөрт хандсан хэрэглэгч, зүйл бүрд эерэг өөрчлөлт авчирсан. Гэвч эдийн засгийн болон бизнесийн орчинд нэлээд хязгаарлагдмал байсаар байна. Петер Штэйнер(Peter Steiner)-ийн 1993 онд бүтээсэн хүүхэлдэйн кинонд нэг нохой нөгөөдөө "Интернетэд чамайг хэн ч нохой гэдгийг мэдэж чадахгүй" гэж хэлдэг бөгөөд энэ үг өнөөдөр ч утга зүйн хувьд алдаагүй ашиглагдаж болохоор байна. Интернет орчинд бид хэн нэгний нэрийг баталгаатай олж авах боломжгүй, эсвэл банк юм уу засгийн газар гэх мэт баталгаат гуравдагч этгээдгүйгээр хэн нэгэнд итгэн мөнгө шилжүүлэх боломжгүй байна. Тэдгээр дундын баталгаажуулан зуучлагч байгууллагууд бидний мэдээллийг цуглуулан, бидний хувийн мэдээлэлд арилжааны ашиг олох болон үндэсний аюулгүй байдал зэрэгт ашиглахаар халддаг. Технологи хувийн мэдээллийг үнэгүйдүүлэхээсээ илүү ашиг орлого авчирдаггүй. Цахин эрин үед, технологи нь бараг л бүх л сайн болон муу зүйлсийн үндсэн цөм болж

байна. Онлайн харилцаа холбоо болон худалдаа зэрэг нь кибер гэмт хэрэгт шинэ боломжийг нээсэн. Моорын хуулиар өнөө цагт процессорын хүчин чадал тодорхой хугацаанд хоёр дахин өсөх нь мөн гэмт хэрэгтнүүд болон хулгайчдын чадлын мөн хоёр дахин өсгөж байна. Гэмт хэрэгтэн болон хулгайчид гэдэгт спам тараагч, хувийн мэдээлэл хулгайлагч, phisher, тагнуулч, zombie farmers, хакер, кибер дарамтлагч болон ransomware тараагч зэрэг орно.

1981 оны эхээр зохион бүтээгчид хувийн мэдээлэл, аюулгүй байдал зэрэг Интернет дэх асуудлуудыг криптографын тусламжтай шийдэл гарцыг хайж эхэлсэн. Тэд үйл ажиллагааг яаж ч инженерчилсэн байсан гуравдагч этгээдийн оролцсон мэдээллийн алдагдал үүссээр байсан. Интернетээр кредит карт ашиглан төлбөр тооцоо хийх нь хэрэглэгч хэтэрхий их хувийн мэдээлэл оруулах шаардлагатайгаас шалтгаалан найдвартай бус, мөн гүйлгээний зардал нь бага хэмжээний төлбөр төлөхөд хэтэрхий их байсан.

1993 онд агуу суут математикч Дэвид Чаум(David Chaum) eCash гэх тоон төлбөр тооцооны системийг танилцуулсан. Энэ систем нь тухайн цаг үедээ интернетээр аюулгүй бөгөөд нэрээ нууцлан төлбөр тооцоо хийх боломжтой бараг л төгс систем болсон. Энэ систем үнэхээр төгс байсан тул Microsoft болон бусад компаниуд eCash - г сонирхож өөрсдийн програмдаа нэвтрүүлсэн. Гэвч асуудал нь тухайн үед интернет худалдан авагчид интернет нууцлал болон аюулгүй байдалдаа төдийлөн анхаардаггүй байсан тул Чаумын герман компани DigiCash 1998 онд дампуурсан.

Энэ явдлаас 10-аад жилийн дараа буюу 2008 онд дэлхийн эдийн засаг хямралд өртсөн. Харин энэ үед Satoshi Nakamoto гэх хуурамч нэртэй хүн эсвэл бүлэг хүмүүс bitcoin гэж нэрлэгдэх криптовалиут ашиглах peer-to-peer электрон төлбөрийн системийн протокол үүсгэсэн. Криптовалиут (дижитал мөнгө) нь аль нэг улсаас үүсгэгдэж, хянагддаггүй гэдгээрээ уламжлалт мөнгөн тэмдэгтээс өөр байсан. Энэ протокол нь сая сая төхөөрөмжүүдийн хооронд итгэмжлэгдсэн гуравдагч талын шаардлагагүйгээр өгөгдөл дамжуулах байдлыг хангаж ажиллах тархсан тооцооллын хэлбэрт тогтсон дүрмийн багц юм. Энэ технологи компьютер тооцооллын ертөнцөд маш сонирхолтой, мөн айдас дагуулсан эсвэл төсөөллийг бодит болгосон мэтээр бизнес, засгийн газар, нийгмийн хөгжлийн хөдөлгөөнүүд, медиа террорист, сэтгүүлчид зэрэг олон салбарт яг л ойн түймэр мэт хурдацтай тархсан.

Энэ протокол нь блокчэйний тархсан дансуудыг нэмэгдэх гол суурь бөгөөд bitcoin-

ий блокчэйн нь хамгийн томд тооцогдож байна. Хэдий технологи нь ойлгоход төвөгтэй боловч үндсэн санаа нь маш энгийн. Блокчэйн нь биднийг бие биедээ шууд бөгөөд аюулгүй мөн банк, кредит картын компани, эсвэл PayPal гэх зэрэг дундын зуучлагчгүй мөнгө дамжуулах боломж олгодог. Энэ технологи нь энгийнээр нээлттэй эхийн програм бөгөөд хэн ч төлбөргүйгээр татаж авч онлайн гүйлгээ хийх шинэ хэрэгсэл хөгжүүлэхэд ашиглаж болох юм.

Анхандаа блокчэйн нь компьютерын шинжлэх ухаанд мэдээллийг хэрхэн зохион байгуулах болон дамжуулах талаарх нэр томьёо төдий байсан. Харин өнөөдөр блокчэйн нь компьютерын хөгжлийн "5 дахь хувьсал" хэмээн өргөмжлөгдөж байна.

Анхны криптографын шифрлэлтээр хамгаалагдсан блокуудын сүлжээг 1991 онд Стюарт Хабер(Stuart Haber) В. Скотт Сторнетта(W. Scott Scornetta) нар танилцуулсан. 1992 онд Баер, Хабер, Сторнетта нар блокчэйнд Merkle trees - г холбосноор нэг блокт хэд хэдэн мэдээллийг цуглуулах боломжтой болж ажлын чадамж нь нэмэгдсэн.

Анхны төвлөрсөн бус блокчэйний концепцыг 2008 онд Сатоши Накамото(Satoshi Nakamoto) гаргаж, дараа жил нь цахим мөнгөн тэмдэгт болох bitcoin - ны цөм хэсэгтэй холбож өгснөөр цахим гүйлгээ бүрд нийтийн данс(ledger) маягаар ашиглах боломжтой болгосон. Peer-to-peer сүлжээ болон төвлөрсөн бус цаг бүртгэлийн серверүүдээр блокчэйний мэдээллийн сан автоматаар зохицуулагдаж байдаг. Bitcoin - д блокчэйнийг ашигласан нь давхар төлөлт буюу цахим гүйлгээнд нэг тоон токен нэгээс илүү ашиглагдах асуудлыг итгэмжлэгдсэн зохион байгуулагчийн шаардлагагүйгээр шийдсэн анхны тоон мөнгөн тэмдэгт болсон.

Блок болон чэйн гэх үгүүд нь Сатоши Накамото - ийн 2008 оны 10-р сарын анхны эрдэм шинжилгээний нийтлэлд салангид бичигдэн хэрэглэгдсэн байсан бөгөөд олон нийтэд алдаршиж блокчэйн гэх нэг үг болтлоо 2016 оныг хүртэл блок чэйн гэх салангид үг байдлаар ашиглагдаж байсан.

2014 онд "Блокчэйн 2.0" нь төвлөрсөн бус өгөгдлийн сангийн блокчэйн програмуудыг илтгэсэн нэршил болж гарч ирсэн. Блокчэйн 2.0 технологи ашигласнаар цахим гүйлгээнд утга солилцоход мөнгө болон мэдээллийн арбитрын үүрэгтэй зуучлагчийн шаардлагагүй болгосон. Хоёрдугаар үеийн блокчэйн технологи хувь хэрэглэгчдийн цахим тодорхойлолт болон хувийн мэдээллийг хадгалах боломжтой болсон.

2016 онд Оросын холбооны сангийн аюулгүй байдлын төв Nxt Блокчэйн 2.0 платформд суурилсан автомат санал хураалтын системийн хэрэглээг судлах туршилтын

төслийг зарласан. Хөгжмийн зах зээлийн төлөөлөл болсон байгууллагууд олноор блокчэйн технологи ашиглан оюуны өмчийн эрхийн шимтгэлийг цуцлуулах, зохиогчийн эрхийг удирдан хянах ажлыг дэлхий нийтээр хэрэгжүүлэх туршилтын загваруудыг туршсаар байна. IMB 2016 оны 7-р сард Сингапур улсад блокчэйний шинэчлэлт болон судалгааны төвөө нээсэн.

2017 оны эхээр Хаврард бизнес шүүмж (Harvard Business Review) сэтгүүлд блокчэйн бол өнөөгийн эдийн засгийн болон нийгмийн системд шинэ үндэслэл бий болгох чадамж бүхий суурь технологи юм гэсэн санал илэрхийлсэн нийтлэл бичжээ.

### 2.1.2 Блокчэйн гэж юу вэ

Блокчэйн гэдэг нь бие даасан хэрэглэгчдийн сүлжээ хооронд цахим мэдээллийн сан үүсгэх болон хуваалцах боломжтой болгох мэдээллийн зохион байгуулалт юм. Блокчэйн нь төвлөрсөн бус өгөгдлийн сангийн технологид шинэ шийдэл болж өгсөн. Энэ шинэчлэлт нь хуучин технологийг шинэ арга замтай холбосноор илүү сайжирч хөгжиж байна. Одоо блокчэйнийг бие даасан хэрэглэгчдийн нэгдэл мэдээллийн санг хадгалж, мэдээллийг хуваалцаж мөн удирдаж ажиллах төвлөрсөн бус өгөгдлийн сан гэж ойлгож болно. Олон төрлийн блокчэйн байдаг:

**Нийтийн блокчэйн** нь давтагдашгүй токенуудаар ажиллах томоохон төвлөрсөн бус сүлжээ юм. Тэдгээр нь аль түвшний хэрэглэгчдэд нээлттэй ба тэдэнд дэмжлэг үзүүлэх нээлттэй эхийн кодууд байдаг.

**Хувийн блокчэйн** нь ихэвчлэн жижиг хэмжээний сүлжээ байхаас гадна токен ашигладаггүй. Хэрэглэгчид нь нарийн хяналт дор үйл ажиллагаа явуулдаг. Энэ төрлийн блокчэйнүүд итгэмжлэгдсэн гишүүд болон нууцлагдсан дамжуулалттай холбоогоор баталгааждаг.

**Зөвшөөрөгдсөн блокчэйн** нь нийтийн болон хувийн блокчэйнүүдийн хосолмол шинжтэй, хувийн блокчэйнтэй ижил хяналттай боловч хянагч нь сүлжээний хэрэглэгч дотроосоо байдаг. Нийтийн блокчэйнтэй ижлээр томоохон төвлөрсөн бус систем байх ба тэдгээр нь давтагдашгүй токен ашиглана. Код нь зарим нь нээлттэй эхийн, зарим нь нээлттэй эхийн бус байдаг.

Дээрх гурван төрлийн блокчэйнууд гурвуулаа криптограф ашиглан аль ч өгөгдсөн сүлжээнээс хэрэглэгч бүрийг төвлөрсөн хянагчийн шаардлагагүйгээр сүлжээнд хэрэгжиж буй дүрмүүдийг хэрэгжүүлэх, данс бүрийг хянах боломжийг олгодог. Төвлөрсөн

хянагчийг өгөгдлийн сангийн бүтцээс халсан нь блокчэйн технологийн хамгийн ашигтай бөгөөд чухал шинж болсон юм.

Блокчэйн хэдий гүйлгээний байнгын бичилт болон түүхийг үүсгэж байдаг ч мөнхийн зүйл гэж байдаггүй. Гүйлгээний бичилтийн байнгын ажиллагаа нь сүлжээний тогтвортой байдлаас хамаардаг. Блокчэйний хувьд энэ нь том хэмжээний блокчэйний нэгдлийн гишүүн нэг бүр мэдээлэлд өөрчлөлт орсныг зөвшөөрөх болон зөвшөөрөхгүй байхыг шийдэж байж эцсийн өөрчлөлт хийгдэнэ гэсэн үг юм.

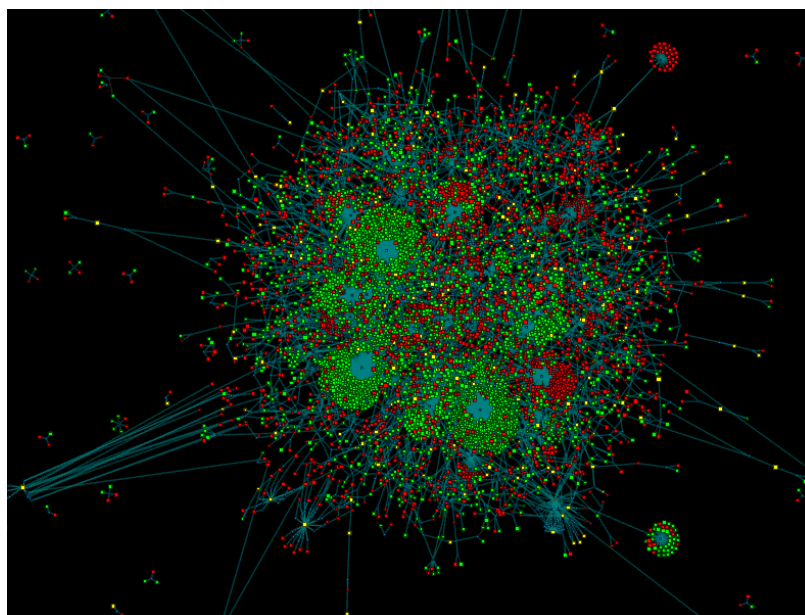
Мэдээлэл блокчэйн нэгэнт бичигдсэн тохиолдолд үүнийг өөрчлөх эсвэл устгах нь бараг боломжгүй зүйл юм. Хэрэв хэн нэгэн блокчэйн бичилт хийх буюу өөрөөр хэлбэл гүйлгээ хийх эсвэл дансны харилцаа хийхийг хүсвэл сүлжээн дэх батлах эрхтэй хэрэглэгчид тухайн захиалсан гүйлгээг баталгаажуулна. Үүнд л блокчэйний хамгийн төвөгтэй хэсэг оршдог учир нь блокчэйн бүр хэн хэрхэн ажиллах, хэн гүйлгээг баталгаажуулах зэргээр бие биеэсээ бага зэрэг өөр үүрэгтэй ажилладаг.

### 2.1.3 Блокчэйн юу хийдэг вэ

Блокчэйн нь ямар нэг мэдээллийн урсгалыг зохицуулагч төвлөрсөн удирдлагагүй peer-to-peer систем юм. Мэдээллийн бүрэн бүтэн, аюулгүй байдлыг хангахын зэрэгцээ төвлөрсөн хяналтыг халах нэг чухал арга нь бие даасан хэрэглэгчид бүхий том хэмжээний төвлөрсөн бус сүлжээтэй байх явдал юм. Ингэснээр тэдгээр компьютерууд тухайн сүлжээг нэгээс олон байршилд байршуулж байна гэсэн үг юм.

Блокчэйн төвлөрсөн бус байдалтай байгаа нь сүлжээний найдвартай байдлыг хангахаас гадна криптовалиутыг ашиглах боломжоор хангах зорилготой. Криптовалиут гэдэг нь дижитал токен бөгөөд зах зээлийн үнэлгээтэй, хувьцааны адилаар мөнгөн дэвсгэртээр арилжаалагддаг.

Криптовалиут нь блокчэйн бүрт бага зэрэг ялгаатай ажилладаг. Ерөнхийдөө техник хангамжуудыг ажиллуулах програм хангамжууд урьдчилан бэлтгэгдсэн байдаг. Тэдгээр програм хангамжууд нь блокчэйний протокол юм. Бидний сайн мэдэх блокчэйн протоколуудад Bitcoin, Ethereum, Ripple, Hyperledger болон Faction зэрэг орно. Зангилаа хэрэглэгчийн техник хангамжийн бүрэлдэхүүн нь сүлжээн дэх мэдээллүүдийг баталгаажуулж байдаг.



About: Visualization of bitcoin transactions (unconfirmed ones).

Node size scale: LINEAR ☐ LOG ☒  
 LEGEND: Green = input, Red = output, Yellow = input+output, Blue = transaction  
 NAVIGATION: mouse + scroll = pan/zoom, SPACE = run/pause  
 TODO:  
 - auto remove transactions older then x min or verified  
 - show transaction details on hover  
 - connect disconnect button  
 - listen for a specyfic address and color it and display alert when present  
 - render graph for specyfic address/transaction  
 - categorise transactions (simple, payments, mixing etc )

Found this interesting :-). Please send some Satoshis here to keep me going:

1NGBYHnYYMli4HZkLsoRy3oFB2DzqusCoU

Зураг 2.1: Блокчэйн сүлжээний бүтэц. Бодит хугацааны хөдөлгөөнт загварыг <http://dailyblockchain.github.io> -с үзэж болно.

#### 2.1.4 Блокчэйн яагаад хэрэгтэй вэ

Блокчэйнийг өнөөдөр компьютерын ухаанд "тав дахь хувьсал" буюу интернетэд өмнө нь байгаагүй "итгэлцлийн түвшин" гэж нэрлэж байна. Энэ нь блокчэйн өнөөдөр дэлхий дахинд маш олон хүний анхаарлын төвд байх гол шалтгаан болж байна.

Блокчэйн цахим мэдээлэлд итгэлцэл үүсгэж байна. Мэдээлэл блокчэйнд нэгэнт бичигдсэн тохиолдолд үүнийг устгах эсвэл засварлах нь бараг л боломжгүй зүйл юм. Энэ боломж нь өмнө нь компьютерын сүлжээний орчинд огт байгаагүй зүйл юм.

Мэдээлэл дижитал хэлбэрт тогтвортой бөгөөд найдвартай байх боломжтой болсон тул өмнө нь гүйлгээний ажлыг зөвхөн онлайн бус горимд хийдэг байсан хэрэглэгчид онлайнаар гүйцэтгэхэд найдвартай итгэж болохуйц болсон. Иргэдийн бүртгэл болон өмчлөх эрх зэрэг уламжлалт үйлчилгээнүүд бүгд онлайн горимд хийгдэж баталгаажих

боломжтой. Банкны гүйлгээ жишээ нь мөнгө шилжүүлэх, орлого зарцуулалт зэрэг хугацаа их шаарддаг ажлуудыг бараг агшин зуурд хийдэг болсон. Аюулгүй, дижитал гүйлгээний бичилт нь дэлхийн эдийн засгийн хувьд асар их ач холбогдолтой зүйл юм.

Анхны блокчэйн аппликэйшнууд өөрийн давтагдашгүй токеноор гүйлгээг баталгаажуулж найдвартай дижитал утгыг гүйлгээгээр дамжуулах нөхцөлөөр хангахаар загварчлагдан бүтээгдэж байсан. Үүнд мөнгө болон хөрөнгийн шилжүүлэлт зэрэг багтдаг. Гэвч блокчэйн сүлжээ нь зөвхөн мөнгөний утгыг дамжуулахаас хол давсан боломжит ирээдүйтэй технологи юм.

### 2.1.5 Блокчэйний бүтэц

Блокчэйн үндсэн гурван цөм хэсгээс бүрддэг :

- **Блок** : Өгөгдсөн хугацаанд гүйлгээний жагсаалт дансанд бичигддэг. Хэмжээ, хугацаа болон блок ажиллах хэмнэл нь блокчэйн бүрд харилцан адилгүй байдаг. Криптовалиутын шилжүүлгийг баталгаажуулах бичилт хийх нь блокчэйн бүрийн хувьд нэн тэргүүний зорилт нь байдаггүй ч блокчэйн бүр криптовалит болон токэн дамжих үйлдлийн бичилтийг хийсээр байдаг. Гүйлгээ гэдгийг энгийнээр мэдээллийн бичилтийг хийх гэж ойлгож болно.

- **Чэйн** : Блокуудыг хооронд нь математикийн ухаанаар хооронд нь холбох хаш утга. Энэ нь блокчэйнийг ойлгоход хамгийн төвөгтэй ойлголт. Чэйн нь мөн блокуудыг нэгтэн байлгаж математикаар итгэл үүсгэж байгаа "шидэт цавуу" юм.

Блокчэйндэх хаш нь өмнөх блокт байсан мэдээллээс үүсдэг. Хаш нь тухайн мэдээллийг блоктэй заавар болон хугацаагаар холбох хурууны хээ болдог.

Блокчэйн нь хаштай харьцуулахад шинэ нээлт юм. Хаш нь 30аад жилийн өмнө бүтээгдсэн. Энэ эртний технологи шинэ технологитой хоршин ажиллаж байгаа шалтгаан нь хаш нь нэг чиглэлт тайлагдах боломжгүй шифр үүсгэдэг. Хаш функц нь мэдээллийг математикийн алгоритм ашиглан ямар ч хэмжээтэй байсан хамаагүй тогтсон хэмжээтэй бит стрингс хэлбэрт оруулдаг. Бит стрингс нь ихэвчлэн 32 тэмдэгтийн урттайгаар мэдээлэл хашлагдсан гэдгийг илэрхийлэхүйц бичиглэлтэй болсон байдаг. Secure Hash Algorithm (SHA) нь блокчэйнд ашиглагддаг криптографын хаш функцийн нэг юм. SHA-256 хамгийн өргөн ашиглагддаг

бараг л дахин давтагдашгүй 256битийн (32байт) -н тогтсон хэмжээт хаш үүсгэдэг. Практик хэрэглээнд хашийг блокчэйнд мэдээллийг байршуулахад ашигладаг дижитал хурууны хээ гэж ойлгож болно.

- **Сүлжээ** : Сүлжээ нь бүрэн зангилаа(Full node)-уудын хэлхээнээс бүрдэнэ. Бүрэн зангилаа гэдгийг сүлжээний эрсдэлийг хариуцах зориулалттай компьютерт ажиллах алгоритм гэж ойлгож болно. Зангилаа бүр тухайн блокчэйнд хийгдэж байсан болон хийгдэж буй бүх гүйлгээний бичилтийг хадгалж байдаг.

Зангилаанууд нь хэн ч байж болох бөгөөд дэлхий даяар тархан байрласан байдаг. Бүрэн зангилааг ажиллуулах нь хүндрэлтэй, өртөг өндөртэй мөн цаг хугацаа их шаардсан ажил тул зангилаа болох хэрэглэгчид үүнийг үнэгүй хийдэггүй. Тэд криптовалит олж авахын тулд зангилааг өөрсдийн компьютер дээрээ ажиллуулдаг. Блокчэйний суурь алгоритм нь зангилаануудад үйлчилгээ үзүүлснийх нь төлөө урамшуулал олгодог. Урамшуулал нь Bitcoin гэх мэт токен болон криптовалит байдаг.

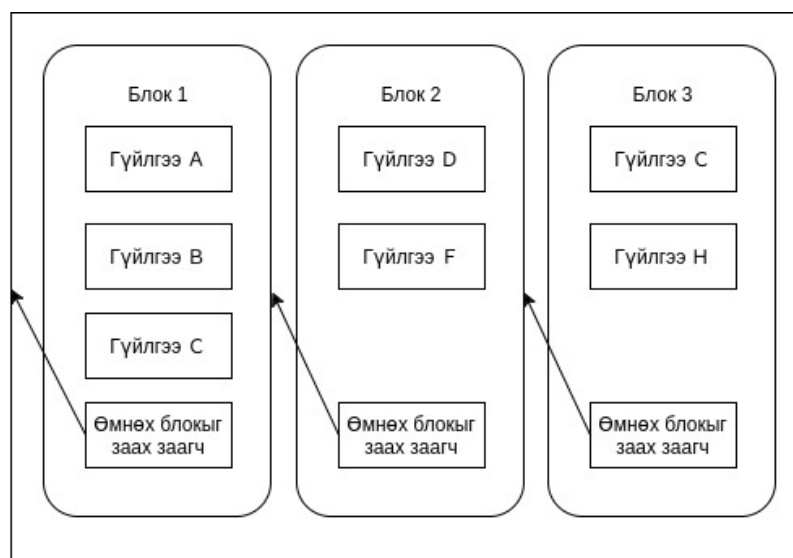
Bitcoin болон блокчэйн гэх ойлголтуудыг ихэвчлэн бие биеэр нь орлуулж нэг утгаар ашиглагдах байдал их гардаг, гэвч энэ хоёр нь тусдаа ойлголт юм. Bitcoin өөрийн блокчэйнтэй. Bitcoin-ий блокчэйн нь bitcoin-ий гүйлгээг найдвартай амжилттай хийгдэх зорилго бүхий суурь алгоритм юм. "Bitcoin" нь Bitcoin сүлжээнд ажиллаж буй криптовалитын нэр бол "Блокчэйн" нь нэг төрлийн програм хангамж юм.

### 2.1.6 Блокчийн гинж (чэйн)

Блокчэйнд энэ шилжүүлгийг гүйлгээ(transaction) гэж нэрлэдэг бөгөөд, олон гүйлгээг багцалсныг блок гэж нэрлэдэг. Гүйлгээ нэг бүрийг зүгээр бүртгээд явбал, нэг мөнгө давхар ашиглагдах "Double spending" хэмээх асуудал үүсдэг. Жишээ нь Батын дансанд 1000 төгрөгийн үлдэгдэл байсан гэе. Нэг зангилаа дээр Батын 1000 төгрөгийг Доржид төлөхөөр боллоо гэж үзье. Гэтэл үүнтэй зэрэгцээд өөр зангилаа дээр Батаас Болдод 1000 төгрөг төлөхөөр боллоо гэж үзье. Зангилаа тус бүр Батын дансны үлдэгдлийг 1000 гэж үзэх учраас, Дорж болон Болд уруу төлөх төлөлтийг зөв гэж үзээд гүйцэтгэхинэ. Батад 1000 төгрөг л байсан боловч, 1000 төгрөгийг 2 удаа ашиглаад 2000 төгрөг ашигласан болж таарна. Энэ асуудлаас зайлсхийхийн тулд гүйлгээ тус бүрд дараалал өгөх шаардлага гарч байна. Жишээ нь Доржид төлөх төлөлт Болдод төлөх төлөлтөөс "өм-



нө” хийгдсэн гэж үзвэл, Болдод төлөх үлдэгдэл хүрэлцэхгүй учраас төлөлт хийгдэхгүй. Блокчэйнд блокийг цаг хугацааны дагуу жагсааж, блок тус бүр 1 өмнөх блокийг зааж байдаг(Блокийн гинж). Ийм байдлаар блокийг нэг эгнээнд оруулсан бүтцээс блокчэйн гэдэг нэр үүсэлтэй юм.



Зураг 2.2: Блокийн гинж буюу чэйн

### 2.1.7 Replicated database

Блокчэйн нь өгөгдлийн сан бүр ижил гүйлгээний утгын жагсаалт хадгалах Replicated database буюу оршуулсан өгөгдлийн сангийн сүлжээ байдлаар ажилладаг. Сүлжээний баталгаажуулагч эсвэл зангилаа гэж нэрлэгддэг сүлжээний гишүүд гүйлгээг нэвтрүүлэх эсвэл зогсоох үйлдлийг хийдэг. Баталгаажуулагч хэрэглэгч бүр тус тусдаа гүйлгээ болон блокийн мэдээллийг шалган нэвтрүүлдэг

Өгөгдлийн санг олшруулна гэдэг нь тухайн нэг компьютер эсвэл сервер дээрх мэдээллийг өөр бусад компьютер эсвэл серверүүдэд хуулбарлаж, тухайн сүлжээний хэрэглэгч бүр ижил хэмжээтэй ижил мэдээлэлтэй болохыг хэлнэ. Ингэж олшруулан тархсан өгөгдлийн сантай болсноор хэрэглэгчид байнга ханддаг чухал мэдээлэлдээ хүрэхийн тулд заавал бусдадаа хандах шаардлагагүй болох юм.

Өгөгдлийн сангийн олшруулалт үндсэн гурван аргаар хийгддэг:

- Snapshot (шуурхай)олшруулалт : Серверт шинэ мэдээлэл ороход тухайн мэдээлэл

өөр нэг серверт эсвэл өөрт байх өөр өгөгдлийн санд тухай тухайн үедээ хуулагдана

- Merging (нэгдсэн) олшруулалт : Хоёр эсвэл түүнээс олон өгөгдлийн сан нэгдэж нэг өгөгдлийн сан болно
- Transactional (гүйлгээний) олшруулалт : Хэрэглэгч өгөгдлийн сангийн мэдээллийг тэр чигт нь хуулж авах бөгөөд авснаас хойш гарсан өөрчлөлтүүдийг тухайн үед нь шинэчилж авна

Тархсан өгөгдлийн сангийн удирдлагын систем нь мэдээллийн аль ч хэсэгт гарсан өөрчлөлт, нэмэлт болон устгалын үйл явцыг хянаж бусад өгөгдлийн сангуудад ижил үйлдлийг хийдэг. Түүнчлэн хэрэглэгч бүр үргэлж бусад хэрэглэгчийн харж байгаа мэдээлэлтэй ижил мэдээллийг харж байдаг.

### 2.1.8 Блокчэйний төрлүүд

Гурван төрлийн блокчэйн байдаг. Үүнд нийтийн сүлжээ (жишээ нь Bitcoin), зөвшөөрсөн сүлжээ (жишээ нь Ripple), хувийн сүлжээ (жишээ нь Hijiго) гурав байна.

- **Public network** буюу нийтийн сүлжээ нь том бөгөөд төвлөрсөн бус, хэн ч аль ч түвшинд нь оролцох боломжтой байдаг. Аль ч түвшин гэдэгт бүрэн зангилаа(full node), криптовалиут олборлолт, токен арилжаа болон утга оруулах зэрэг багтдаг. Энэ төрлийн сүлжээ нь хувийн болон зөвшөөрөгдсөн сүлжээгээ бодвол арай илүү аюулгүй найдвартай байдаг. Гэвч ихэвчлэн удаан бөгөөд ашиглахад зардал өндөртэй. Криптовалиутаар хамгаалагдах ба хадгалах багтаамж нь хязгаарлагдмал байдаг.
- **Permissioned network** буюу зөвшөөрсөн сүлжээ нь нийтэд ил боловч оролцогч нь удирдагдаж байх ёстой. Ихэнх нь криптовалиутад ашиглагддаг ч сүлжээн дээр суурилсан аппликэйшнуудад бага зардалтай ажиллах боломжтой. Энэ чанар нь төсвийг бууруул бөгөөд гүйлгээний цар хүрээг өсгөхөд тустай. Энэ төрлийн блокчэйнууд нийтийн сүлжээнээс илүү хадгалалтын багтаамжтай байх ба хоцрогдол багатай маш хурдан ажилладаг
- **Private network** буюу хувийн сүлжээ нь итгэмжлэгдсэн оролцогчдын дунд байх бөгөөд нийтэд ил бус байж болно. Энэ сүлжээ асар хурдан барагтаа хоцрогдолгүй ажиллана. Түүнчлэн маш бага зардлаар ажиллах бөгөөд шахуу ажиллавал

долоо хоногийн дотор бүтээгдэнэ. Ихэнх хувийн сүлжээ нь криптовалюта ашигладаггүй бөгөөд төвлөрсөн бус сүлжээнээс өөр аюулгүй байдлын бодлоготой байдаг. Хадгалалтын багтаамж нь хязгааргүй.

Эдгээрээс гадна энэ гурван үндсэн төрлийн нэгтгэсэн хосолмол байх ба энэ нь аюулгүй байдал, хяналт, сүлжээг өргөтгөх боломж болон сүлжээн дээрх апплиэйшнийг хадгалах багтаамж зэргийн хамгийн ашигтай балансыг олохын тулд судлагдаж байгаа.

### 2.1.9 Блокчэйний хөгжлийн үе шат

Блокчэйн bitcoin үүсэхтэй зэрэгцэн үүсэн хөгжсөн. Энэхүү сүлжээнд хоорондоо хэзээ ч уулзаж байгаагүй бүлэг хүмүүс нэг системд бие биедээ итгэн хамтран ажиллаж болдог гэдгийг нотолсон.

**Анхны Bitcoin сүлжээ** нь Bitcoin криптовалютын найдвартай байдлыг хангахаар бүтээгдсэн. Дэлхийгээр төвлөрсөн бус 5000 орчин бүрэн зангилаанаас бүрдэж байсан бөгөөд bitcoin арилжаалах болон утга шилжүүлэхэд гол зорилго нь оршиж байсан ч хэрэглэгчид энэ сүлжээнд үүнээс ч илүү боломж байгааг олж харсан. Сүлжээний далайц болон аюулгүй байдал зэргээс шалтгаалж бусад жижиг блокчэйнүүд болон блокчэйн аппликэйшнуудыг хамгаалахад ашиглагдах болсон.

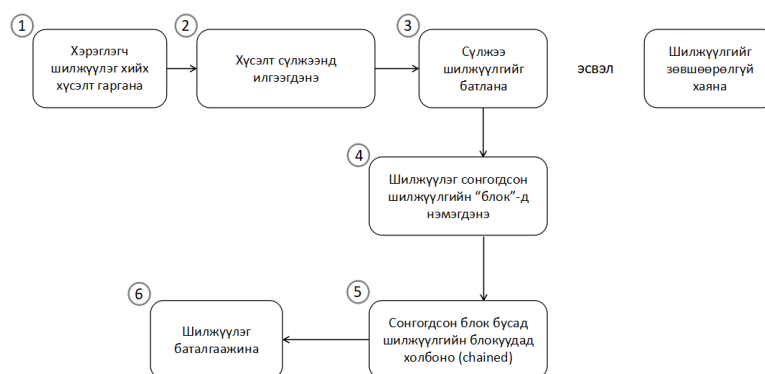
**Ethereum сүлжээ** нь блокчэйн концепцын хоёр дахь хөгжлийн үе юм. Уламжлалт блокчэйн бүтцийг ашиглахаас гадна үүн дотор програмын хэл оруулж өгсөн. Bitcoin - той адилаар дэлхийгээр төвлөрсөн бус 5000 орчим бүрэн зангилаанаас бүрдэнэ. Ethereum -ийн үндсэн зорилго нь Ether - г арилжаалах, ухаалаг гэрээ (smart contract) хийх, төвлөрсөн бус автомат байгууллага(DAOs) бүтээх байсан. Bitcoin - ий адилаар жижиг блокчэйнүүд болон блокчэйн аппликэйшнүүдийн найдвартай байдлыг хангахад мөн ашиглагддаг.

**Factom сүлжээ** нь блокчэйн технологийн гурав дахь үе юм. Санал хураалтын систем агуулсан, мөн илүү их хэмжээний мэдээлэл агуулах багахан хэмжээний нэгдмэл сүлжээг ашигладаг. Мэдээлэл болон системийн аюулгүй байдлыг хангах зорилгоор бүтээгдсэн. Нэгдсэн зангилаанууд болон хязгааргүй тооны хянагч зангилаатайгаар ажилладаг. Сүлжээ нь жижиг тул төвлөрсөн бус сүлжээнд холбогдож хадгалагч блокчэйнүүдээ холбон ажилладаг.

## 2.1.10 Тохиролцооны алгоритм

Блокчэйн нь системийн дүрмийг хэрэгжүүлэхэд гуравдагч этгээдийн оролцоо шаардлагагүй найдвартай систем юм. Сүлжээний дүрмийг хэрэгжүүлэхэд үндсэн тохиролцооны (consensus) алгоритмыг ашигладаг.

Блокчэйний хувьд үндсэн тохиролцоо гэдэг нь итгэмжлэгдээгүй зангилаануудын хооронд тохиролцоо үүсгэх процесс юм. Тэдгээр нь сүлжээний бүрэн зангилаа (full nodes) байдаг бөгөөд дансны нэг хэсэг болон бичигдэж байгаа гүйлгээ бүрийг баталгаажуулдаг.



Зураг 2.3: Блокчэйн хэрхэн ажиллах загвар

Блокчэйн бүр сүлжээндээ өгөгдөл оруулахад тохиролцоо үүсгэх алгоритмтай. Блокчэйн бүр өөр төрлийн өгөгдөлтэй байдаг тул тохиролцоог үүсгэх олон төрлийн загвар байдаг. Зарим блокчэйнууд нь утга солилцдог бол зарим нь мэдээллийг ангилж, зарим нь систем болон гэрээний аюулгүй байдлыг хангадаг.

Жишээ нь Bitcoin - ний хувьд өөрийн сүлжээн дэх хэрэглэгчдийн хооронд токены утгыг дамжуулдаг. Токенууд нь зах зээлийн ханштай тул гүйцэтгэлийн чадал, далайц, найдвартай байдал, аюул болон алдааны эсрэг байдлын шаардлага нь өндөр байдаг. Bitcoin нь халдагчид гүйлгээний түүхийг өөрчлөх эсвэл токен хулгайлахыг оролдох зэрэг байнгын аюул дор үйл ажиллагаа явуулдаг. Bitcoin эдгээр аюулаас сэргийлэхийн тулд **"proof of work"** гэж нэрлэгддэг тохиролцоог ашигладаг. Энэ тохиролцоо нь Byzantine - ий үндсэн асуудал болох "Чиний харж байгаа мэдээлэл дотоод болон гадаад талаасаа өөрчлөгдөөгүй гэдгийг яаж мэдэх вэ?" гэдэгт шийдэл болдог. Мэдээлэлд өөрчлөлт оруулах, гуйвуулах асуудал нь компьютерын шинжлэх ухаанд аль ч үед

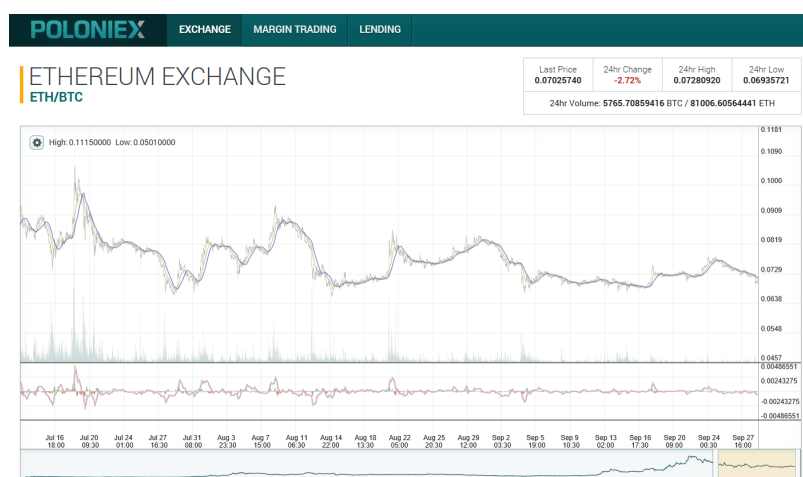
бараг л хэзээд боломжтой асуудал байсаар ирсэн.

Ихэнх блокчэйнууд гадаад нөлөөлөл болон системийн дотоод хэрэглэгчдээс халдлагад өртөх магадлалын дор ажиллаж байдаг. Ирж болох халдлагууд болон хэрэглэгчдийн сүлжээний найдвартай байдлын зэрэг нь сүлжээнд үйл ажиллагаа явуулж буй зангилаануудын өөрсдийнх нь дансаа тохируулахдаа сонгон ашигласан тохиролцооны алгоритмаас хамаардаг. Жишээ нь Bitcoin болон Ethereum өөрсдийгөө халдлагад өртөх өндөр магадлалтай гэж үзвэл **"proof of work"** алгоритмыг ашиглаж болно.

Нөгөө талаас баталгаажсан цэгүүдийн хооронд мөнгөн гүйлгээний бичилт хийдэг блокчэйнууд энгийн бөгөөд хурдан ажиллагаатай тохиролцоог ашиглах боломжтой. Тэдний хувьд хурдан хугацаанд гүйлгээ хийх нь илүү чухал. Proof of work нь тэдний хувьд сүлжээнд нь харьцангуй цөөн хэрэглэгч байхаас гадна гүйлгээ бүр шуурхай хийгдэх шаардлагатайгаас шалтгаалж үйл ажиллагаа явуулахад хэтэрхий удаан бөгөөд зардал өндөртэй.

### 2.1.11 Блокчэйн хэрэглээнд

Өнөөдөр дэлхий даяар маш олон блокчэйн болон блокчэйний апплицэйшнүүд оршиж байна. Дэлхий нийтээр мөнгөний гүйлгээг шуурхай хийх, төвлөрсөн бус сүлжээнд хувь нийлүүлэх болон удирдах, мөн аюулгүй техник хангамж болон аппликэйшн бүтээхэд анхаарлаа хандуулж байна.



Зураг 2.4: Криптовалиут арилжааны платформ

Блокчэйнууд дан ганц арилжааны утга дамжуулахаас давж бүх төрлийн салбарт оролцож эхэлсэн. Блокчэйн өмнө нь байгаагүй найдвартай байдлыг онлайнд ажиллах орчинд үүсгэж байна.

### 2.1.12 Өнөөгийн блокчэйний хэрэглээ

Өнөөдрийн ихэнх амжилттай ажиллаж байгаа блокчэйн аппликэйшнууд нь түргэн шуурхай, хямд өртгөөр мөнгө болон бусад төрлийн утга дамжуулах зориулалттай аппликэйшнууд байна. Үүнд хувьцаат компаниудын хувьцаа арилжаалах, олсон улсын ажилчдадаа цалин өгөх, мөн нэг мөнгөн тэмдэгтийг өөр мөнгөн тэмдэгтээр солих зэрэг багтана.

Блокчэйн мөн програм хангамжийн аюулгүй байдлын багцын хэсэгт ашиглагдаж байна. Америкийн бүс нутгийн аюулгүй байдлын яам (U.S Department of Homeland Security) Зүйлсийн Интернет(Internet of Things) - н аюулгүй байдлыг хангах блокчэйн програмуудыг санхүүжүүлж байсан. Зүйлсийн интернет нь гаднаас чагнах болон бусад төрлийн халдлагад өртөх өндөр магадлалтай байсан тул блокчэйн технологиос хамгийн их боломж хүртсэн салбаруудын нэг болсон юм. Зүйлсийн интернет төхөөрөмжүүд илүү сайжирч, аюулгүй байдал нь үлэмж баталгаажсан. Тэдгээрийн жишээ нь эмнэлгийн систем, өөрийгөө жолоодох машин, болон аюулгүй байдлын системүүд юм.

DAO нь мөн маш сонирхолтой шинэ санаануудын нэг юм. Энэ төрлийн блокчэйн аппликэйшнууд нь компаниудыг онлайнаар нэгтгэн зохицуулах шинэ шийдэл болсон. DAO өмнө нь Ethereum сүлжээгээр зохицуулалт болон хөрөнгө оруулалтаа хийдэг байсан.

### 2.1.13 Блокчэйн аппликэйшн ирээдүйд

Улсын хэмжээнд газрын бүртгэл хийх, иргэдийн бүртгэл болон олон улсын зорчигч тээврийн аюулгүй байдлыг хангах програмуудын туршилт дээрх томоохон урт хугацааны судалгааны ажлууд хийгдэж байна. Их Британи, Сингапур, Арабын Нэгдсэн Эмират Улс зэрэг орнууд блокчэйнийг зардал бууруулсан шинэ төрлийн эдийн засгийн хэрэгсэл гэдэг талаас нь харж байгаа бөгөөд идэвхтэй хөрөнгө оруулалт болон судалгаа хийсээр байна.

Математик тэгшитгэлээр "итгэлцэл"гэх зүйл үүсгэснээр блокчэйн шаардлагатай салбарууддаа хүрч чадсан. Өмнө нь "итгэлцэл"гэх зүйл нь зарим салбарт ахадсан зүйл

байсан бол блокчэйн үүссэнээр энэ нь байх боломжтой зүйл болсон. Түүнчлэн "итгэлцэл"гэх зүйл үгүй болсон газарт дүрэм сахиулах салбарынхны ажлыг хөнгөвчилсөн. Утгат суурилсан болон нийгэмд суурилсан гүйлгээг бид хэрхэн хийж байгаагаас хамаарч блокчэйн өөрчлөгддөг тул блокчэйн аппликэйшны нийгмийн болон эдийн засгийн ойлголт нь сэтгэл хөдлөлийн болон улс төрийн туйлшралд өртөж байна.

#### 2.1.14 Блокчэйнийг хүрээлэн буй орчин

Аппликэйшн хөгжүүлэлтийн гол талбар байгууллага доторх компьютероос (on-premise software) үүлэн технологи (cloud) уруу шилжсэнтэй адилаар, блокчэйнийг бас хэд хэдэн үүлэн орчинд ашиглах боломжтой.

Голлох үйлчилгээ нь IBM-н хөгжүүлж буй Hyperledger-ийн үүлэн үйлчилгээ “IBM Bluemix Blockchain” болон Microsoft-ийн үзүүлдэг Ethereum үүлэн үйлчилгээ “Microsoft Azure Blockchain as a Service (BaaS)”, Sakura Интернетийн Tech Bureau-тай хамтран үзүүлдэг NEM-д суурилсан mijin үүлэн үйлчилгээ “mijin cloud service beta” зэрэг юм.

Аль ч үйлчилгээ нь, хугацааны хувьд харилцан адилгүй ч, тодорхой хэмжээнд үнэгүй ашиглах боломжтой учраас блокчэйн ашиглаж үзье гэвэл энэ мэт үүлэн үйлчилгээнүүдийг ашиглах боломжтой.

Цаашид иймэрхүү чиглэлийн үйлчилгээ улам эрчимжиж, блокчэйнийг хүрээлсэн орчин улам бүр төгөлдөржих байх гэж харагдаж байгаа.

#### 2.1.15 Технологи болон хууль, эрх зүй

Блокчэйний хөгжүүлэлт хийх орчин улам төгөлдөржихийн хамт, хийсвэр мөнгө талаасаа, харамсалтай нь мөнгө угаалтанд ашиглагдах, гэмт хэрэгт ашиглагдах зэрэг нь мөн ихэссээр байна. 2016 оны 5 сард Японд хийсвэр мөнгөний тухай хууль батлагдсан.

Уг хууль хэрэгжиж эхлэхээр, хийсвэр мөнгө “Төлбөрийн хэрэгсэл болгон ашиглаж болох хөрөнгө” гэж тодорхойлогдсон бөгөөд (ердийн марк болон кредит карттай адилаар) хийсвэр мөнгийг хууль ёсны мөнгөн тэмдэгттэй солих үед татвар ногдуулахгүй болох юм.

Мөн уг хуульд, хийсвэр мөнгийг хууль ёсны мөнгөн тэмдэгттэй солих үйл ажиллагааг бүртгүүлсэн хуулийн этгээд явуулах бөгөөд суурь хөрөнгийн талаарх шаардлага болон үйл ажиллагааны явц дахь мэдээллийн хяналт, тогтмол шалгалт зэргийг нарийн дүрмүүдээр зааж өгсөн байна.

## 2.2. ТӨВЛӨРСӨН БУС СҮЛЖЭЭ (DECENTRALIZED NETWORK) БҮЛЭГ 2. ОНОЛ

### 2.1.16 Блокчэйний боломжууд

Блокчэйнийг цаашид ямар салбарт хэрэглэгдэхээр харагдаж байгаа талаар танилцуулъя. Эхний хэрэглээний салбар бол, bitcoin гол төлөөлөл нь болж буй криптовалиут юм.

Уламжлалт банк санхүүгийн байгууллагаар дамжуулж гүйлгээ хийх нь төвөгтэй шат дамжлагатай мөн шимтгэл өндөртэй, хугацаа их шаарддаг. Блокчэйн ашигласан хийсвэр мөнгөний хувьд ийм дундын зуучлагч шаардахгүйгээр гүйлгээ хийх боломжтой бас гүйлгээний шимтгэл бага, цаг хугацаа хэмнэдэг. Ялангуяа улс хооронд мөнгө илгээхэд дээрх давуу талуудыг мэдрэх болно. 2015 оны байдлаар, дэлхий даяар илгээж буй мөнгөн дүн ойролцоогоор 60 их наяд иентэй дүйцэхүйц том зах зээл байна.

Дараагийн салбар нь баримт бичгийн баталгаажуулалт (нотариат) юм. Засах боломжгүй гэдэг шинж чанарыг ашиглан, блокчэйн дээр баримт бичиг, эсвэл баримт бичгийн хаш утгыг хадгалснаар, тэрхүү баримт бичиг нэг цаг үед байсан, мөн тухайн үеийн агуулга нь өөрчлөгдөөгүй гэдгийг баталж чадна.

Эстониа улсад, гэрлэлтийн баталгаа, гэрээслэл, газар эзэмшлийн гэрчилгээ зэргийг блокчэйн дэд хадгалснаар, уламжлалт нотариатыг орлох оролдлого хийж байна. Мөн тус улсад хувь хүний эмчилгээний түүх үрүү хандах хандалтад блокчэйн дэд суурилсан технологийг ашиглаж байна.

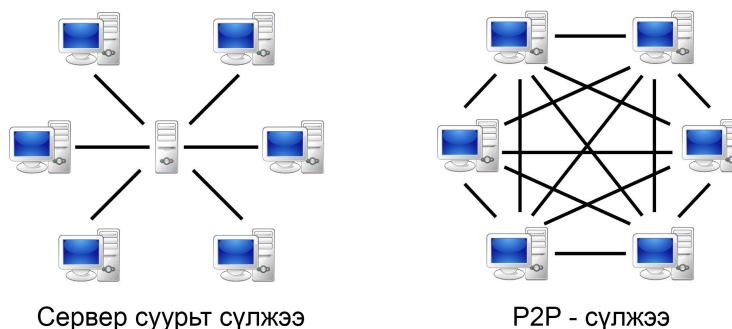
Технологиос гадна, хууль эрх зүйн хүрээнд ч бас өөрчлөлт орж байна. Ялангуяа Fintech-ийн хувьд олон компани хүчээ үзэж байна.

## 2.2 Төвлөрсөн бус сүлжээ (Decentralized network)

Компьютеруудыг хэрэглэх хандлага зонхилох үед персонал компьютерууд дотоод сүлжээгээр дамжин төв сервертэй холбогддог байсан. Эдгээр серверүүд маш их өгөгдөл боловсруулдаг учир персонал компьютероос хүчин чадлын хувьд маш өндөр байсан. Түүнээс хойш персонал компьютер хүчирхэг болсоор ойр орчмын төв серверүүдээс өгөгдлийг боловсруулахдаа илүү болсон. Яагаад гэвэл PC-ээс PC-рүү эсвэл төвлөрсөн бус тооцоолол нь хувийн компьютерыг төв серверийг тойрч бусад компьютеруудтай шууд хамтран ажиллах боломжийг хангаж чаддаг. Клиент серверийн аль аль нь хүсэлт илгээх эсвэл үйлчилгээ үзүүлэх эсэхээс хамаардаг бол төвлөрсөн бус систем дэх бүх зангилааг зиндаа нэг гэж авч үздэг. Өөрөөр хэлбэл нэг клиент нь нөгөөгөөсөө мэдээлэл авч байхад нөгөө клиент эргүүлээд мэдээлэл тэгш эрхтэйгээр өгч байна гэсэн үг



ЮМ.



Зураг 2.5: Peer to peer сүлжээ болон сервер суурьт сүлжээний топологи

Peer-to-peer (P2P) сүлжээ нь хэрэглэгч зангилаа бүр ижил эрхтэй мөн аль ч зангилаа нь холболтын горим үүсгэх боломжтой төвлөрсөн бус сүлжээний загвар юм. Клиент нь үйлчилгээний хүсэлт илгээж, сервер нь хүсэлтийг биелүүлэх клиент/сервер загвараас ялгаатай нь P2P сүлжээнд зангилаа бүр клиент болон серверийн хоёр үүргийг давхар гүйцэтгэдэг.

P2P сүлжээний загвар нь клиент/сервер сүлжээний загвараас дараах байдлаар ялгаатай:

- Контентууд болон нөөцүүд хэрэглэгч бүрд ижил хуваагддаг, харин клиент/сервер загварын хувьд зөвхөн төв компьютер дээр байрладаг
- P2P сүлжээ нь сервер суурьт сүлжээтэй харьцуулахад илүү найдвартай, сүлжээний ашиглалт өндөртэй
- P2P сүлжээн дэх компьютерууд ганц сервер компьютероос хамааралгүйгээр өөрсдөдөө байгаа нөөцөө хувааж тархсан тооцооллын боловсруулалтыг хийнэ
- P2P сүлжээний компьютер нь сүлжээн дэх өөр компьютероос хэрэгцээт мэдээллээ ямар нэг серверээр дамжилгүйгээр шууд татаж авах боломжтой

P2P систем нь сүлжээний урсгал, их хэмжээний параллель тооцооллын орчин, тархсан хадгалах төхөөрөмжүүд болон бусад үйл ажиллагаанд нууц чиглүүлэлт үүсгэхэд ашиглагддаг. Ихэнх P2P програмууд аудио, видео мэдээлэл болон бусад бүх төрлийн

## 2.2. ТӨВЛӨРСӨН БУС СҮЛЖЭЭ (DECENTRALIZED NETWORK) ҮҮЛЭГ 2. ОНОЛ

дигитал форматаар бичигдсэн файл солилцох, харилцаа холбоонд ашиглагдах, мэдээлэл хуваалцахад төвлөрсөн байдаг, гэвч P2P-тэй холбоотой програм хангамжийн нууцлал болон зохиогчийн эрхийн зөрчлүүд их гардаг.

Ерөнхийдөө peer-to-peer програмууд хэрэглэгчдэд үйл ажиллагааны олон параметруудийг удирдах боломжоор хангадаг, жишээ нь : тухайн агшинд хэдэн холболтод хандах эсвэл нэвтрүүлэх, хэний системийг холбох эсвэл хязгаарлах, ямар үйлчилгээг санал болгох, мөн сүлжээнд хэдэн системийн нөөцийг ажиллуулах гэх мэт.

P2P сүлжээний топологи нь ARPANET - ийн үеэс судлагдаж ирсэн хэдий ч 1990 - д оны сүүлээр Napster гэх мэт дуу хуваалцах програмууд гарч P2P холболтын загварын давуу тал нийтэд танигдаж интернетийн сүлжээнд ашиглагдаж эхэлсэн. Napster болон түүний Gnutella гэх мэт залгамжлагчид мөн BitTorrent зэрэг програмууд дуу хөгжим болом киноны зах зээлийн ашигт шууд нөлөөлж хүмүүсийн мэдээллийг эзэмших болон хэрэглэх хандлагад илт өөрчлөлт хийсэн.

Napster, OpenNap болон IRC@find гэх мэт сүлжээ болон сувгууд нь зарим үйлдэлдээ (хайлт гэх мэт) клиент/сервер бүтцийг ашигладаг. Gnutella, Freenet зэрэг сүлжээнүүд бүрэн P2P загвартай гэгддэг ч бусад зангилаануудын байршлыг тодорхойлох лавлах(directory) сервер ашигладаг.

Төвлөрсөн бус тооцооллын систем нь peer-to-peer сүлжээнд ажилладаг. Төвлөрсөн бус P2P сүлжээ гэдэгт, сүлжээнд оролцогч буюу зангилаа нь газарзүйн хувьд тархсан байдаг ба зангилаа хооронд мэдээлэл солилцоо нь агшин зуур хийгддэггүй, тархах байдлаар явагддаг учраас “төвлөрсөн бус” гэдэг утгыг, мөн зангилаа нь сервер зэргээр дамжилгүйгээр өөр зангилаа-тэй шууд холбогддог “P2P(peer to peer)” гэдэг утгыг агуулж байдаг.

Төвлөрсөн бус P2P сүлжээнд гүйлгээг баталгаажуулахын тулд, зангилаа хоорондын мэдээлэл солилцоо шаардлагатай болно. Дээрх мөнгө шилжүүлэх жишээн дээр мөнгө шилжүүлэлт зөв явагдсан эсэхийг баталгаажуулахын тулд, хэнд хэчнээн төгрөг байгаа вэ гэдэг мэдээллийг сүлжээнд байгаа бүх зангилаа дээр мэдэж байх хэрэгтэй.

Тодорхойгүй тооны олон оролцогчтой сүлжээнд, мэдээллийг солилцохдоо, тэдгээр мэдээллийг засах эрсдэлтэй биш үү, ялгаатай зангилаа дээр ялгаатай үр дүнд хүрвэл яаж нэгдсэн нэг үр дүнд саналаа нэгтгэх вэ гэдгийг бодох шаардлагатай гарч байна.

Peer-to-peer сүлжээ нь голдуу физик сүлжээний топологи дээр виртуал бүрхэх сүлжээний (Overlay network) зарим загварыг хэрэгжүүлдэг. Мэдээллүүд үндсэн TCP/IP

## 2.2. ТӨВЛӨРСӨН БУС СҮЛЖЭЭ (DECENTRALIZED NETWORK) БҮЛЭГ 2. ОНОЛ

сүлжээн дээгүүр дамжуулагдсаар байдаг ч application layer-т peer-үүд логик бүрхэх холбоосоор хоорондоо шууд холбогдож харилцдаг. Давхаргууд нь peer олох болон индексжүүлэх, мөн P2P системийг физик сүлжээний топологиос хамааралгүй болгоход ашиглагддаг. Зангилаанууд давхарга сүлжээгээр бие биетэйгээ хэрхэн холбогдсон байдал, мөн нөөцүүд хэрхэн индексэжсэн болон байршсан байдлаас шалтгаалж бүтэцлэгдсэн болон бүтэцлэгдээгүй сүлжээ гэж ангилдаг(эдгээр хоёрын хосолмол бүтэцтэй байдаг). Gnutella, FastTrack гэх мэт P2P сүлжээнүүд нь бүтэцлэгдээгүй сүлжээ юм.

### **Төвлөрсөн бус сүлжээ нь дараах давуу талуудтай**

- Суурилуулах болон тохируулахад хялбар
- Холбогдсон компьютерууд нь серверээс хамаарахгүй
- Хувь хэрэглэгчид өөрсдийн хамтран хуваалцаж буй эх сурвалжийг хянаж чадна
- Худалдан авах болон байгуулахад үнэтэй биш
- Сүлжээний тусгай програм хангамж шаарддаггүй
- Сүлжээнд ажиллах тусгай администратор шаардахгүй

### **Төвлөрсөн бус сүлжээ нь дараах сул талуудтай**

- Сүлжээний хамгаалалт нь зөвхөн тухайн эх сурвалжид тухайн цаг хугацаанд хамаарна
- Хэрэглэгчид эх сурвалж болгонд өөр өөр олон нууц үг өгдөг.
- Холбогдсон компьютер болгон өөрийн эх сурвалжаа хамгаалах шаардлагатай

### **2.2.1 Төвлөрсөн бус сүлжээний архитектур**

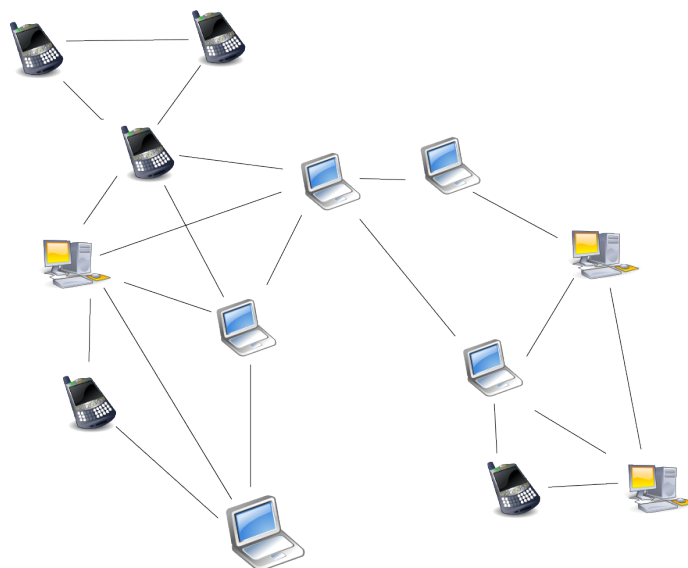
Peer-to-peer сүлжээ нь голдуу физик сүлжээний топологи дээр виртуал бүрхэх сүлжээний (Overlay network) зарим загварыг хэрэгжүүлдэг. Мэдээллүүд үндсэн TCP/IP сүлжээн дээгүүр дамжуулагдсаар байдаг ч application layer-т peer-үүд логик бүрхэх холбоосоор хоорондоо шууд холбогдож харилцдаг. Давхаргууд нь peer олох болон индексжүүлэх, мөн P2P системийг физик сүлжээний топологиос хамааралгүй болгоход ашиглагддаг. Зангилаанууд давхарга сүлжээгээр бие биетэйгээ хэрхэн холбогдсон байдал,

## 2.2. ТӨВЛӨРСӨН БҮС СҮЛЖЭЭ (DECENTRALIZED NETWORK) БҮЛЭГ 2. ОНОЛ

мөн нөөцүүд хэрхэн индексэжсэн болон байршсан байдлаас шалтгаалж бүтэцлэгдсэн болон бүтэцлэгдээгүй сүлжээ гэж ангилдаг(эдгээр хоёрын хосолмол бүтэцтэй байдаг). Gnutella, FastTrack гэх мэт P2P сүлжээнүүд нь бүтэцлэгдээгүй сүлжээ юм.

### 2.2.1.1 Бүтэцлэгдээгүй сүлжээ

Бүтэцлэгдээгүй peer-to-peer сүлжээ нь загварын хувьд бүрхэх сүлжээн дээр тодорхой бүтцийг байгуулдаггүй, харин зангилаанууд хоорондоо санамсаргүй байдлаар холболт үүсгэж зохион байгуулалтад ордог. (Gnutella, Gossip, Kazaa зэрэг нь бүтэцгүй P2P протоколын жишээ юм)



Зураг 2.6: Бүтэцлэгдээгүй P2P сүлжээний загвар

Бүтэцлэгдээгүй сүлжээнүүдийн дээгүүр дахин шинэ бүтэц нэмэгдэхгүй тул байгуулахад амар бөгөөд давхаргын өөр өөр байршилд зохион байгуулах боломжтой. Түүнчлэн сүлжээн дэх бүх реер-үүдийг үүрэг оролцоо ижил учир бүтэцлэгдээгүй сүлжээ нь маш олон тооны реер-үүд ойр ойрхон сүлжээнд холбогдох болон гарах үе гэх мэт ачаалал өндөртэй үед маш бат бөх байж чаддаг.

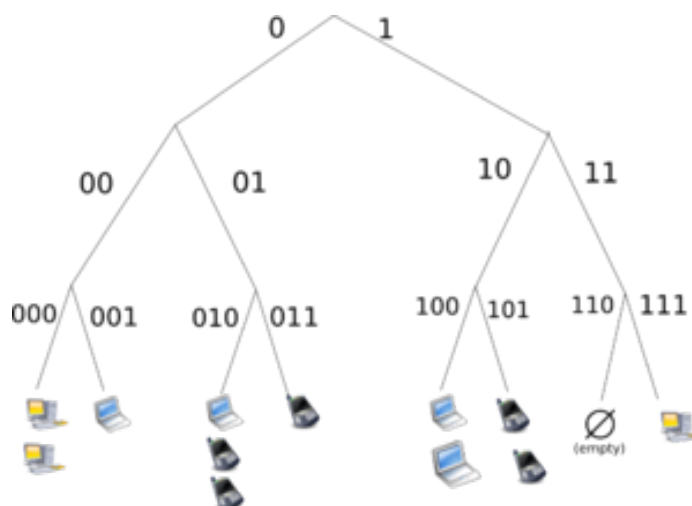
Бүтцийн дутагдалтай байдлаас шалтгаалж бүтэцлэгдээгүй сүлжээнд зарим хязгаарлагдмал байдлууд бий болдог. Тухайлбал, сүлжээн дэх реер мэдээллийн тодорхой нэг хэсгийг олох хэрэгцээ гарвал, хайлтын хүсэлт сүлжээн дэх тухайн мэдээллийг агуулж болох аль болох олон реер - үүдээр урсаж гарна. Энэ урсгал нь сүлжээнд маш их хэм-

## 2.2. ТӨВЛӨРСӨН БУС СҮЛЖЭЭ (DECENTRALIZED NETWORK) БҮЛЭГ 2. ОНОЛ

жээний сигналын ачаалал үүсгэж CPU/memory - н ачааллыг нэмэгдүүлдэг ч хайлтын хүсэлт үргэлж амжилттай биелнэ гэсэн баталгаа байдаггүй. Түүнчлэн реер-үүдийн хооронд ямар ч харилцан хамаарал байдаггүй тул тухайн хайлтын урсгал хүсэж буй мэдээлэл нь хадгалагдаж байгаа реер-ээ олно гэх баталгаа мөн байдаггүй. Олон реер-үүдэд хадгалагдаж буй түгээмэл файлууд олдох магадлал өндөр байдаг бол хэдхэн реер-т байгаа мэдээллийг хайхад олдох үр дүн маш бага байдаг.

### 2.2.1.2 Бүтэцлэгдсэн сүлжээ

Бүтэцлэгдсэн сүлжээ нь давхарга тодорхой топологи болох зохион байгуулагддаг, мөн протокол нь сүлжээнд аль ч реер хүссэн файл болон нөөцийг хэдий маш ховор байсан ч үр ашигтайгаар хайж олох баталгааг хангадаг.



Зураг 2.7: Бүтэцлэгдсэн P2P сүлжээний загвар

Хамгийн өргөн ашиглагддаг бүтэцлэгдсэн P2P сүлжээний төрлүүд нь хайж байгаа мэдээллээ хэн эзэмшиж байгааг тодорхойлох зорилгоор ашигладаг бүрэлдэхүүнт хаш (consistent hashing) - н төрөл болох distributed hash table (DHT) - г ашигладаг. DHT - д хадгалагдаж буй хослол(түлхүүр, утга)-н hash table - г ашиглан сүлжээний нөөцийг олох боломжтой болгодог, мөн ямар ч идэвхтэй зангилаа үр ашигтайгаар өгөгдсөн түлхүүрт нийцэх утгыг буцаана.

Сүлжээний үр ашигтай байдлыг хангахын тулд бүтэцлэгдсэн сүлжээн дахь зангилаанууд тухайн нөхцөлийг хангасан хөршийн жагсаалтыг дэмждэг байх ёстой. Ингэс-

нээр сүлжээний өндөр ачаалалтай үед зангилаануудыг тэсвэр багатай болгодог. Бодит ачааллын үе дэх P2P нөөц олох шийдэлд хийсэн тооцооллоор нөөц зарлах/илрүүлэх ачаалал өндөр, мөн статик болон динамик ачааллын тэнцвэр алдагдах зэрэг ДНТ - д суурилсан хэд хэдэн асуудлыг илрүүлсэн.

### 2.2.1.3 Хосолмол загвар

Хосолмол загвар нь peer-to-peer сүлжээ болон клиент-сервер загварын хослол юм. Нийтлэг хосолмол загвар нь реер-үүд нэг нэгнээ олоход зориулагдсан төвлөрсөн сервертэй байдаг. Энэ төрлийн загварын томоохон жишээ нь Spotify юм. Маш олон тооны хосолмол загварууд байдаг бөгөөд тэдгээр нь бүгд бүтэцлэгдсэн клиент/сервер сүлжээгээр загварчлагдсан төвлөрсөн үйл ажиллагаагаар тохиролцож, харин реер-үүд бүтэцлэгдээгүй цэвэр peer-to-peer сүлжээгээр хангагддаг. Одоогийн байдлаар хосолмол загвар нь төвлөрсөн үйл ажиллагаат хайлттай бөгөөд зангилаанууд нь бүтэцлэгдээгүй сүлжээний төвлөрсөн бус үйл ажиллагааны давуу талыг ашигласан нь цэвэр бүтэцлэгдсэн болон цэвэр бүтэцлэгдээгүй сүлжээний загваруудаас харьцангуй илүү гүйцэтгэлтэй байж чадаж байна.

## 2.3 Нууцлал аюулгүй байдал

### 2.3.1 Хаш функц

Хаш функц нь блокчэйн технологийн үндсэн суурь хэсэг юм. Хэрэв хаш функцийг ойлгочихвол хорт үйлдлийг илрүүлэх (tamper proof), тоон хурууны хээ зэрэг бусад концепцуудыг ойлгоход хялбар болно.

Хаш концепц нь үнэндээ маш энгийн. Энэ технологийг тайлбарласан техникийн хэл нь л хүмүүсийн толгойг эргүүлдэг. Хаш функцийг энгийнээр тайлбарлавал энэ нь тодорхой нэг оролтын утгыг авч гаралтын утга үүсгэдэг функц юм.

Энэ тодорхойлолтыг дэлгэрүүлбэл, хаш функц ямар ч хэмжээтэй утгыг оролтдоо аваад тогтмол урттай гаралтын утга үүсгэдэг.

MD5 гэж нэрлэгддэг хаш функцийн нэг төрлөөр жишээ авъя:

Үүнд авсан стрингс утгаа санамсаргүй тоо болон үсгээс бүрдсэн “a0680c04c4eb53884be77b4e1067” гэх гаралтын утга болгон гаргасан байна. Энэ үйлдлийг **мэдээллийг хураангуйлах** (message digest) гэж нэрлэдэг. Түүнчлэн **тоон хурууны хээ** ч гэж нэрлэгдэх нь бий.

```
cloudnthings:bin cloudnthings$ echo "I owe my sister $5" | md5
a0680c04c4eb53884be77b4e10677f2b
cloudnthings:bin cloudnthings$
```

Зураг 2.8: MD5 -аар хашлах үйлдэл

Дээрх жишээн дэх “I owe my sister \$5” гэсэн оролтын утгын зөвхөн ганц тэмдгийг өөрчлөх буюу жишээ нь “I owe my sister \$2” болгоход гаралтын утга нь тэр чигтээ өөрчлөгдөх болно.

### 2.3.2 Хаш функцийн төрлүүд

Олон төрлийн хаш функц байдаг. Блокчэйний хувьд үндсэн ашигладаг хаш функц нь SHA256 болон RIPEMD. 128 эсвэл 256 гэх тоонууд нь үндсэндээ гаралтынхаа утгын уртыг илэрхийлдэг. SHA256 нь 256бит утга гаргана гэсэн үг.

```
[pi@raspberrypi:~ $ echo -n "I owe my sister $5" | sha256sum
5d0838314e62443e929c6794a0d2a566a23a69fa614243bfe20e8ca651e955b0
```

Зураг 2.9: SHA256 гаралтын утга

Дээрх зурагт SHA256 командыг Линукс дээр ажиллуулаад гаралтдаа 256бит буюу 64 тэмдэгтийн урттай болсон байна.

### 2.3.3 Өөрчлөлтийг илрүүлэх

Ирсэн мэдээллийг замдаа өөрчлөгдсөн эсэхийг мэдэх хамгийн амар арга нь илгээгчийн мэдээллийн гаралтын хаш утгыг ирсэн мэдээллийн хаш утгатай харьцуулах юм. Хэрэв хаш утгууд яг ижил байвал мэдээлэл алдаагүй иржээ гэдэгт итгэлтэй байж болно.

### 2.3.4 Давхцал

Маш олон хүмүүс мэдээллийн хураангуй хэзээ ч давхцахгүй байх боломжтой юу гэдэгт эргэлзэн, хэзээд дахин давтагдашгүй байна гэдэг боломжгүй гэж үздэг.

Мэдээж гаралтын утга тогтсон урттай тул хязгааргүй тооны дахин давтагдашгүй утга байна гэж байхгүй ч энэ технологийн нууц нь хоёр өөр утга ижил хаш гаралттай байх тохиолдлыг олохын тулд бүх компьютеруудыг ашиглахад хэдэн арван сая жил

шаардагдана. Иймд энэ технологи ойрын ирээдүйн хэрэгцээнд хангалттай баталгаатай гэсэн үг юм.

### 2.3.5 Нэг чиглэлт функц

Өөр нэг хаш функцийн чухал шинж нь нэг чиглэлт үйлдэл хийдэг. Энэ нь мэдээллийг хураангуйлахад маш хялбар боловч хураангуйллыг эргэн тайлах нь бараг л боломжгүй зүйл юм. Өмнөх жишээ шиг мэдээж огт боломжгүй биш боловч гаралтын утгыг олоход мөн л асар их хугацаа шаардана.

### 2.3.6 Шахалт

Хаш функцийн бас нэг ойлголт нь шахалт. Том хэмжээтэй өгөгдөл стрингсээр илэрхийлэгдэх маш богино өгөгдөл болон гардаг. Үүнийг мэдээлэл дамжуулалтын явцад алдаа гарсан, эсвэл өөрчлөлт орсон зэргийг илрүүлэхэд ашиглаж болдог.

### 2.3.7 Хаш функц блокчэйнд хэрхэн хэрэглэгддэг вэ

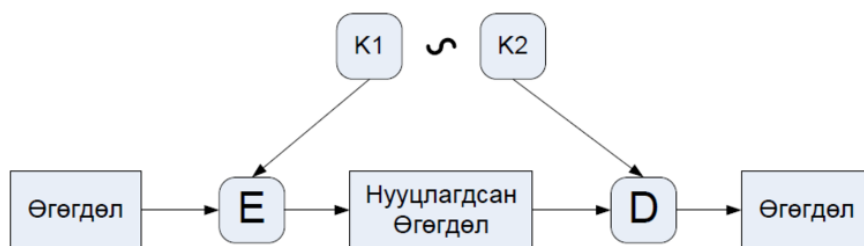
Блокчэйн үйл ажиллагаандаа хаш функцийг байнга ашигладаг. Блокчэйн дахь мэдээллүүд блок бүрд хашлагдсан байдаг. Хэрэв блок өөрчлөгдвөл, жишээ нь хэн нэгэн өөрт байгаа bitcoin -ий хэмжээг өөрчлөх, эсвэл хэн нэгэнд хэр өртэй гэдгээ өөрчлөхийг оролдвол хаш утга нь өөрчлөгдөөд бусад блок бүр ямар нэг өөрчлөлт гарсныг тэр дороо мэднэ.

Өмнөх блокийн хашлагдсан утгыг шинэ блокийн хаш утгыг үүсгэхэд ашигладаг тул блокуудын холбоо үүсдэг.

### 2.3.8 Нийтийн түлхүүртэй нууцлалын алгоритм

Нийтийн түлхүүрийг харилцагч бүр мэддэг байх ба хувийн түлхүүрийг ганцхан өөртөө хадгалах ёстой. Нийтийн болон хувийн түлхүүрүүд нь бие биенээсээ харилцан хамааралтай хосолмол шинжтэй байдаг. Аливаа нэг хосын хувийн түлхүүр өөр нэг хосын нийтийн түлхүүртэй зохицон ажиллах боломжгүй. Нийтийн түлхүүрийг бусдад түгээхдээ шууд файл хэлбэрээр дамжуулах, нийтийн түлхүүр хадгалах сервер дээр байршуулах зэрэг аргууд ашигладаг. Хувийн түлхүүрийг бол зөвхөн өөрийн компьютерт хадгална.





Зураг 2.10: Нийтийн түлхүүртэй алгоритм

### 2.3.9 RSA алгоритм

RSA нь интернет дээгүүр хувийн болон нууц мэдээлэл дамжуулахад өгрөн ашиглагддаг нийтийн түлхүүрээр мэдээллийг нууцлах крипто-систем юм. RSA-г 1978 онд Массачүсетийн Технологийн хүрээлэнгийн (Massachusetts Institute of Technology) R.Rivest, A.Shamir, L.Adelman нар бүтээсэн. Нийтийн түлхүүрт шифрлэлт буюу ассиметрик шифрлэлт нь нэг нийтийн болон нэг хувийн хоёр өөр боловч математикийн уялдаатай түлхүүрүүд ашигладаг. Нийтийн түлхүүр нь бүгдэд нээлттэй бол хувийн түлхүүр нь нууц байх ёстой. RSA шифрлэлтэд нийтийн болон хувийн түлхүүрүүд хоёул зурвасыг шифрлэх боломжтой. Энэ шинж нь RSA алгоритмыг хамгийн өргөн ашиглагддаг ассиметрик алгоритм болгосон.

RSA алгоритм нь өнөөгийн мэдээлэл технологийн хамгаалалтын гол тулгуур болж байна. Интернетээр худалдаа хийх үед хөтчийн веб хаягийн өмнөх цоожны зураг онлайн дэлгүүртэй хийж буй харилцаа шифрлэгдсэн байгааг илэрхийлнэ. Цоожны зурган дээр даралт хийж, дэлгэрэнгүй мэдээлэл дотроос тоо болон үсгүүдийн дарааллыг харж болно. Энэ нь 16-тын тооллоор илэрхийлэгдсэн хэн ч харж болох нийтэд дэлгэсэн түлхүүр юм. Кредит картын дугаарыг оруулах үед нийтэд ил харагдах түлхүүр автоматаар дуудагдаж, дугаарыг шифрлэн дэлгүүрт илгээдэг. Ил түлхүүр үнэхээр аюулгүй байж чадах уу гэсэн эргэлзээ төрнө. Үүний нууц нь зөвхөн нэг чиглэлт функцийн үр дүн юм. Бид телефон утасны жагсаалтаас хүний нэрээр утасны дугаарыг олж болох ч, эсрэгээр дугаараас нэрийг олж болдоггүйтэй адил юм.

RSA алгоритм анхны тоог ашигладаг. Анхны тоо нь 1, 3, 5, 7, 11 гэх мэтчилэн хязгааргүй үргэлжилнэ. Эрдэмтэд 2500 жилийн туршид бүхий л анхны тоог нэгэн зэрэг илэрхийлэх нэгдсэн томъёог хайсаар ирсэн боловч олж чадаагүй л байна. Энэ нь анхны тоог шифрлэлтэд ашиглах үндэс болжээ. Дэлгүүр хэрэглэгчийн мэдээллийг нууц-

лахын тулд урьдчилан 2 анхны тоог сонгодог. Тэдгээрийн үржвэр нь нийтэд үзүүлэх түлхүүр болно. Кредит картын дугаар энэ түлхүүрээр шифрлэгдэн илгээгдэж, дэлгүүр анхны 2 тоог мэдэх учир шифрийг тайлж кредит картын дугаар уншигдана. Нөгөө талаас хакерууд түлхүүрийг анхны тооны үржвэрт задалж чадвал кредит картын дугаарыг мэдэж чадах мэт санагдана. Гэвч энэ нь боломжгүй юм. Одоогийн байдлаар RSA шифрлэлтийн түлхүүр нийт 617 оронгоос бүрдэж байна. Энэ нь өнөөгийн ямар ч супер компьютер, хэдэн ч ширхгийг ашигласан үржвэрийг олох боломжгүй том тоо юм.

RSA алгоритмыг Америкийн Үндэсний Стандартчиллын Газар (NIST)-аас PKCS1, ANSI X9.31, IEEE 1363 стандартуудаар баталгаажуулсан байдаг бөгөөд мэдээллийн жижиг блокуудыг шифрлэх, түлхүүр солилцох үйлдлийг ашигладаг програм хангамжууд болон SSH, OpenPGP, S/MIME, болон SSL/TLS зэрэг маш олон протоколуудад, мөн тоон гарын үгийн загварт хэрэглэгдэж байна.

RSA алгоритмын түлхүүрийг 512бит, 1024бит, 2048бит, 4096бит урттайгаар сонгон авч болдог. Төсөөлбөл 64, 128, 256, 512 үсэгтэй нууц үг байна гэж ойлгож болно. Ийм урт нууц үгийг цээжлэх хэцүү. Тиймээс нууц үгийг файл дээр бичээд компьютерт хадгалдаг. Нийтийн түлхүүрийг харилцагч бүр мэддэг байх ба хувийн түлхүүрийг ганцхан өөртөө хадгалах ёстой. Нийтийн болон хувийн түлхүүрүүд нь бие биенээсээ харилцан хамааралтай хосолмол шинжтэй байдаг. Аливаа нэг хосын хувийн түлхүүр өөр нэг хосын нийтийн түлхүүртэй зохицон ажиллах боломжгүй. Нийтийн түлхүүрийг бусдад түгээхдээ шууд файл хэлбэрээр дамжуулах, нийтийн түлхүүр хадгалах сервер дээр байршуулах зэрэг аргууд ашигладаг. Хувийн түлхүүрийг бол зөвхөн өөрийн компьютерт хадгална. RSA алгоритмаар ямар ч хэмжээний өгөгдлийг нууцалж болно. Өгөгдлийг нийтийн түлхүүрээр нууцалж, хувийн түлхүүрээр тайлна. RSA алгоритмын давуу тал нь өгөгдлийг нууцлах болон баталгаажуулах чадвартай байдаг. Нууцлах бол бидний мэддэгээр баримт бичгийг бусад хүмүүс гартаа оруулсан ч унших боломжгүй болгохыг хэлнэ. Харин баталгаажуулах нь баримт бичигт тамга даран баталгаажуулдаг шиг тийм үйлдлийг тоон баримтад хэрэгжүүлдэг. Үүнийг тоон гарын үсэг гэж нэрлэн заншжээ. RSA алгоритмыг тоон гарын үсэг, сертификатад голлон ашиглаж байна.

RSA нийтийн түлхүүр нь  $(n, e)$  гэсэн бүхэл тоон хосоос бүрдэх ба энд RSA модуль  $n$  нь ижил битийн урттай санамсаргүйгээр үүсгэсэн (нууц)  $p, q$  хоёр анхны тоонуудын үржвэр байна. Өөрөөр хэлбэл  $n = p * q$ . Шифрлэх илтгэгч нь :

$$1 < e < \varphi(n), \text{ ged}(e, \varphi(n)) = 1$$

нөхцөлийг хангах бүхэл тоо, энд  $\varphi(n) = \varphi = (p-1)(q-1)$ . Хувийн түлхүүр  $d$ -ийг мөн шифр тайлах илтгэгч гэж нэрлэх ба

$$1 < d < \varphi(n), \text{ ed} \equiv (\text{mod} \varphi)$$

нөхцөлийг хангах бүхэл тоо байна.  $(n, e)$  нийтийн түлхүүрээс хувийн түлхүүр  $d$ -ийг тодорхойлох бодлого нь  $n$  тооны  $p, q$  үржвэрүүдийг тодорхойлох бодлоготой тооцооллын хувьд нэг болохыг баталсан. Аливаа том тоог анхны тоонуудын үржвэрт задлах асуудал нь тооцооллын хувьд хүнд бодлого юм.

### 2.3.10 Цахим гарын үсэг

Тоон гарын үсэг нь мэдээллийн эх үүсвэрийн үнэн зөв байдлыг баталгаажуулахын тулд, мөн тухайн мэдээлэл бүрэн бүтэн байгааг нотлон шалгахад мэдээллийн хүлээн авагчид эрх олгодог. Иймээс нийтийн түлхүүрт тоон гарын үсэг нь танилт болон өгөгдлийн бүрэн бүтэн байдлыг хангадаг. Тоон гарын үсэг нь гар бичмэлийн гарын үсэгтэй ижил зорилготой. Гэсэн хэдий ч, гар бичмэлийн гарын үсэг нь хуурамчаар үйлдэхэд хялбар байдаг. Тоон гарын үсэг нь гар бичмэлийн гарын үсгийг бодвол бараг л хуулбарлах боломжгүйгээс гадна мэдээллийн агуулгууд болон гарын үсэг зурагчийг жинхэнэ байдлыг нотолдог бөгөөд дараах 2 зүйлийг баталгаажуулдаг мэдээлэл юм. Үүнд:

- Цахим баримт буюу файлд гарын үсэг зурсан этгээд буюу эзэн, хариуцагч нь хэн бэ гэдгийг
- Тухайн файлд гарын үсэг зурагдсанаас хойш санаатай болон санамсаргүй байдлаар ямар нэгэн өөрчлөлт ороогүй эсвэл эвдрээгүй гэдгийг

Зарим тохиолдолд, энэ мэдээллийг тухайн файлаас нь салгах боломжгүйгээр түүнд хавсаргасан байдаг. Өөрөөр хэлбэл, ямар нэгэн файл үүсгэхэд түүний нэр, хэмжээ, төрөл, үүсгэсэн, өөрчилсөн огноо зэрэг мэдээлэл нь файлын агуулгад биш гэхдээ дайвар байдлаар тухайн файльтайгаа хамт байдагтай адил зүйл. Дараах зүйлсийг тоон гарын үсэгт тооцохгүй. Жишээлбэл:

- Ямар нэгэн материал дээр үзгээр гарын үсгээ зураад тухайн материалаа скайндэж эсвэл фото зургийг нь авч цахим хэлбэрт оруулсан хуулбар

- Зурмал гарын үсэг бүхий факс
- Ямар нэг баримтын агуулга дотор скайндаж оруулсан, зурмал гарын үсгийн зураг
- Цахим шууданд хавсаргасан, зурмал гарын үсгийн зураг гэх мэт

Эдгээр нь тоон гарын үсэгтэй ямар ч хамааралгүй, зүгээр л нэг файл, дүрс, тэмдэгт бөгөөд хүмүүсийн ихэнх нь эдгээр хэлбэрийг тоон гарын үсэг гэж бодож төөрөлддөг. Харин эдгээр арга, хэлбэрийг тоон гарын үсгийн мөрөөдлийн, зөгнөлт хэлбэр гэж үзэх нь бий. Үнэн хэрэгтээ, эдгээр мэдээлэл нь тухайн баримтын үнэн худал болон хариуцагчийг бүрэн баталгаажуулдаггүй тул хүчин төгөлдөр гарын үсэг хэмээн тооцож ашиглах боломжгүй юм. Хэн нэгний нийтийн түлхүүрийг ашиглан мэдээллийг шифрлэхийн оронд, та өөрийн хувийн түлхүүрээрээ шифрлэх хэрэгтэй. Хэрэв тухайн мэдээлэл таны нийтийн түлхүүрээр тайлагдан уншигдах боломжтой байвал тэр нь танаас үүсгэгдсэн мэдээлэл байх ёстой.

Өдөр тутмын амьдралд файл болон бичиг баримтыг илгээж, хүлээж авахдаа хүлээж авсан файл үнэхээр зөв хүнээс илгээгдэж ирсэн эсэхийг баталгаажуулж чадахгүй байж болох юм.

Жишээ нь Бат Доржид чухал материал илгээх тохиолдолд, муу санаатай хэн нэгэн Батын оронд өөр материал илгээж магадгүй, эсвэл Батын явуулсан материалыг замаас нь хулгайлж, засварлаад Доржид явуулж магадгүй. Энэ үед Доржийн хүлээж авсан файл “Батаас илгээсэн зөв файл мөн” гэдгийг хэрхэн шалгах вэ. Энэ асуудлыг шийдэж өгөх арга нь цахим гарын үсэг юм.

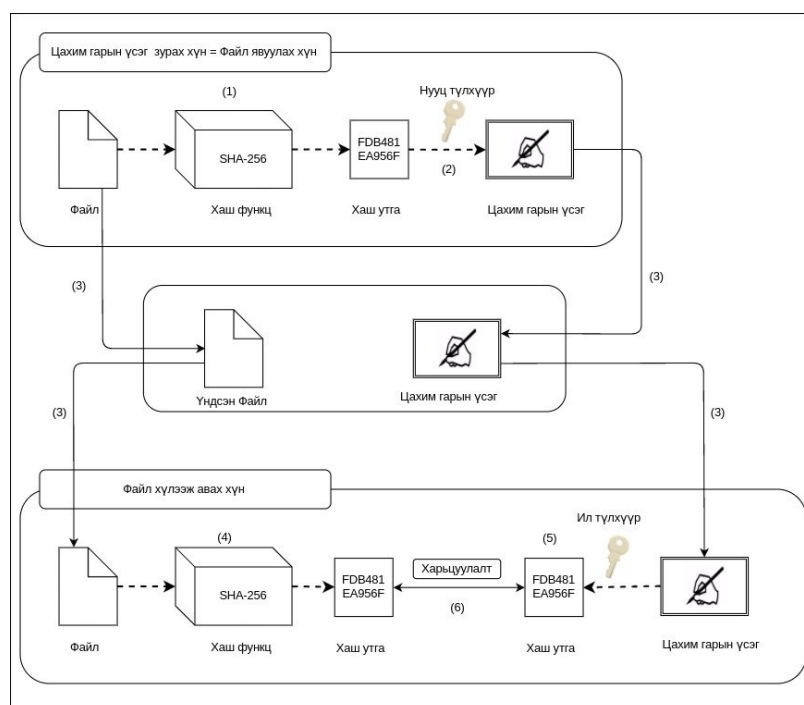
Дээрх жишээ шиг олон тохиолдолд файл болон бичиг баримтыг илгээх үед, хүлээж авагч нь тухайн файлыг илгээгч нь үнэн зөв илгээгч байсан, бичиг баримт нь мөн үнэн зөв, засварлагдаагүй байсан гэдгийг баталгаажуулах шаардлагатай.

Цахим гарын үсгээр, түлхүүрийн хослолыг(нууц болон нийтэд ил) ашиглан, гарын үсгийг үүсгэж, гарын үсгийг шалгаснаар дээрх шаардлагыг хангадаг. Нууц түлхүүр нь гарын үсэг гэж нэрлэгддэг бөгөөд, гарын үсэг зурах хүнд л байна. Харин, нийтэд ил түлхүүр нь шалгалтын түлхүүр гэж нэрлэгддэг бөгөөд, хэн ч олж авах боломжтой байдлаар нийтэд ил болгосон байдаг. Нууц түлхүүр болон нийтэд ил түлхүүр нь дараах онцлогуудтай.

- Нууц түлхүүрээр нууцалсан өгөгдлийг зөвхөн ил түлхүүрээр задлах боломжтой

- Ил түлхүүрээр нууцалсан өгөгдлийг зөвхөн нууц түлхүүрээр задлах боломжтой

Ил түлхүүрээр нууцалсан өгөгдлийг зөвхөн нууц түлхүүрээр задлах боломжтой Ил түлхүүрээр нууцлах нь “Интернет дэлгүүрт кредит картын мэдээлэл илгээх”, “Нэвтрэх нууц үг илгээх” зэрэгт ашиглагддаг. Харин, нууц түлхүүрээр нууцалсан өгөгдөл нь зөвхөн, нууц түлхүүртэй хүн л нээнэ гэдэг чанарыг ашиглаж “хэн задалсан бэ” гэдгийг нь баталгаажуулах арга(цахим гарын үсэг) болгон ашигладаг. Батаас Доржид бичиг баримт илгээх тохиолдлыг жишээ болгон цахим гарын үсгээр явуулахыг Цахим гарын үсэгтэй файл явуулах урсгал-д үзүүлээ.



Зураг 2.11: Цахим гарын үсэгтэй файл явуулах урсгал

1. Бат (Гарын үсэг зурах = нууц түлхүүртэй хүн) үндсэн файлын хаш утгыг тооцоолно.
2. Батын нууц түлхүүрээр олсон хаш утгыг кодлоод, түүнийг гарын үсэг гэж үзнэ.
3. Батаас үндсэн файл болон гарын үсгийг Доржид илгээнэ.
4. Дорж хүлээж авсан файлаас хаш утгыг нь бодож олно.

5. Дорж хүлээж авсан гарын үсгийг Батын нууц түлхүүрт харгалзах ил түлхүүрээр задалж, үндсэн файлд харгалзах хаш утгыг олж авна.
6. Дорж 4-т бодож олсон “үндсэн файлын хаш утга” болон 5-д задалж олсон “үндсэн файлын хаш утга”-г харьцуулна.
7. Уг харьцуулалтаар 4 болон 5-ууд ижилхэн байвал уг файл Батаас явуулсан файл мөн бөгөөд ямар нэг засваргүйгээр хүлээж авсан гэдгийн баталгаа болно.

Ийм байдлаар, цахим гарын үсэгт хаш функц болон хос түлхүүрийг нийлүүлж ашигласнаар, өгөгдөл илгээгчийг болон агуулгын засагдаагүй гэдгийг баталгаажуулах ажлыг зэрэг гүйцэтгэдэг юм. Блокчэйнд өмнөх хэсгийн хаш функц болон дээр өгүүлсэн цахим гарын үсгийг аль алийг нь ашигладаг бөгөөд гүйлгээ тус бүрийн үнэн зөв байдал, нийцтэй байдлын талаарх мэдээллийн илгээгч, агуулгын бүрэн бүтэн(засагдаагүй) байдлын баталгаа зэрэг төрөл бүрийн зорилгоор ашигладаг.

## 2.4 Тохиролцооны протоколууд

Өмнө хэлсэнчлэн, блокчэйн бол блок тус бүрийг нэг эгнээнд жагсаасан бүтэцтэй байдаг. Оролцох бүх зангилаа дээр ижил мэдээлэл бүхий блок ижил дарааллаар жагссан байх шаардлагатай. Уг блокийн дарааллыг шийдэх арга болгож блокчэйнд янз бүрийн нийцтэй байдлын алгоритмыг ашигладаг. Жишээлбэл, PoW(Proof of Work), PoS(Proof of Stake), PoI(Proof of Importance), PBFT(Practical Byzantine Fault Tolerance)

### 2.4.1 PoW(Proof of Work)

PoW бол bitcoinд ашиглагддаг алгоритм бөгөөд ерөнхийдөө майнинг/mining/ гэж нэрлэгддэг үйл ажиллагаанд хийгддэг зүйл юм. PoW-оор блок дотор агуулагддаг гүйлгээний мэдээлэл болон өмнөх блокийн хаш утган дээр санамсаргүй тоо(nonce) нэмж, хаш утга тооцоолоод явна. Бодож олсон хаш утга урьдчилан тохируулсан шалгуур утгаас бага болтол нь санамсаргүй тоог өөрчилж, дахин тооцоолол хийнэ. Нөхцөлд таарах хаш утгыг олбол, уг блокийг идэвхтэй блок болгож, оролцогчдод түгээж, хүлээн зөвшөөрүүлнэ.

Хүлээн зөвшөөрөх тал нь хүрч ирсэн блоконд агуулагдах санамсаргүй тоо болон мэдээлэл тус бүрийн хаш утгыг зөвхөн нэг удаа тооцоолж үнэхээр блокчэйний нөхцө-

лийг хангаж байгаа эсэхийг шалгана. Энэ үед хийгдэх шалгах(тооцоолох) процесс нь зөвхөн нэг удаа хийгдэх бөгөөд майнинг хийхэд явагддаг их хэмжээний тооцоололтой харьцуулахад маш богино хугацаанд тооцон шалгаж болдог гэдгээрээ онцлогтой.

Bitcoin-д урьдчилан тохируулсан нөхцөлд таарсан блокийг үүсгэж чадсан нөхцөлд, блок үүсгэгчид урамшуулал болгон BTC/bitcoin/-г өгдөг.

Одоогийн байдлаар 1 блок үүсгэлтээр олж авах урамшуулал 12.5 BTC учраас хувь хүнд ногдох урамшуулал гэдэг утгаараа маш өндөр мөнгөн дүн юм. Bitcoin-д энэ мэтийн урамшууллаар мотивацилагдаж, хаш тооцооллын өрсөлдөөн явагдаж байдаг.

Нэмж хэлэхэд, bitcoin-ы майнингид Sha256 гэдэг алгоритм ашиглагддаг бөгөөд энэ алгоритмд зориулан оптимизаци хийгдсэн ASIC(Application Specific Integrated Circuit) гэдэг зориулалтын цахилгаан хэлхээ ашигласнаар өндөр хурдны майнинг хийх боломжтой болдог. Хаш утгын бодолтыг илэрхийлэх үзүүлэлт болгож хашрэйт(хаш үүсгэсэн тоо/секунд) ашиглагддаг бөгөөд 2017 оны 3 сарын байдлаар bitcoin систем бүхэлд нь авч үзвэл хашрэйт 3,252PH/s(Petahash/second) байдаг бөгөөд маш өндөр тооцон бодох чадвартай болохыг харж болно.

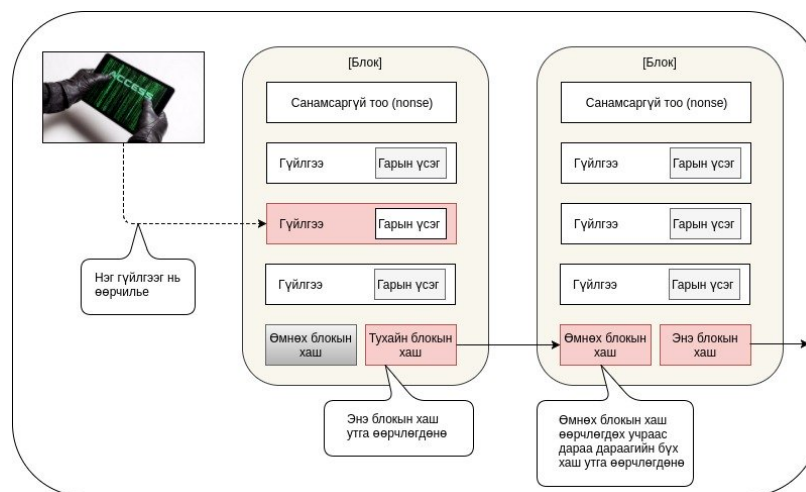
Харьцуулалт болгож, Intel Core i7 5820K бүхий CPU-гээр майнинг хийсэн тохиолдолд хашрэйт нь ойролцоогоор 10MH/s учир, хувь хүн CPU-гээр майнинг хийсэн нөхцөлд блок үүсгэх магадлал 325 тэрбумд 1 болох юм. Солир таарах магадлал 10 тэрбумын нэг гэж нэрлэгддэг учраас бодит байдал дээр CPU-гээр хожихгүй гэдэг нь тодорхой.

Bitcoin-д блокийг зэрэг олох магадлал байж болох учир олон газарт зэрэг олдсон тохиолдолд гинж салалт үүсэх болно. Ийм тохиолдолд, “Хамгийн урт гинж бүхий салаа нь хамгийн их хэмжээний тооцооллын зардлаар олдсон” гэдэг зарчим дээр тулгуурлаж, хамгийн урт гинж бүхий салааг сонгож авна гэсэн байдлаар явагдана. Хамгийн урт гинжийг сонгож авах арга нь гинжийг өөрчлөх асуудлын хувьд ч хамгаалалт болох үр нөлөөтэй.

Жишээ нь, хорон санаалсан хэрэглэгч, нэг блок дахь гүйлгээний агуулгыг өөрчилъё гэж үзсэн тохиолдлыг бодож үзье(Гүйлгээний мэдээллийг зассан үед).

Энэ тохиолдолд, гүйлгээний агуулгыг өөрчлөх учраас блокийн хаш утга бас өөрчлөгдөнө. Блокийн хаш утга өөрчлөгдмөгц, өмнө нь хангаж байсан нөхцөл (хаш утга шалгуур утгаас бага)-ийг хангаж чадахгүй болох учраас дахин санамсаргүй тоог өөрчилж, таарах хаш утгыг олох шаардлага үүснэ.

Энэ блок нь гинжний толгой хэсгээс /гинжний хамгийн шинэ, сүүлд нэмэгдсэн хэ-



Зураг 2.12: Гүйлгээний мэдээллийг зассан үед

сэг/ бусад тохиолдолд, дараагийн блокод энэ блокийн хаш утга ашиглагдаж байгаа учраас, дараагийн блокийн хаш утгыг мөн өөрчилж бичих шаардлага үүснэ. Ингэмэгц, ээлж дараалан хаш утгыг дахин тооцоолж, хаш утгуудыг өөрчилж бичих шаардлага үүсч, энэ нь гинжний толгой/гинжний хамгийн шинэ, сүүлд нэмэгдсэн хэсэг/ хүртэл үргэлжлэх хэрэгтэй болно. Засъя гэж бодсон блокоос блокийн эхэн/гинжний хамгийн шинэ, сүүлд нэмэгдсэн хэсэг/ хүртэлх өөрчлөх хурд(өөрчлөгчийн тооцон бодох resource) нь жинхэнэ гинжний өсөх хурд (bitcoin системийн бүх тооцон бодох resource)-г давж гараагүй тохиолдолд уг дайралт амжилтгүй болох учраас гинжний өөрчлөлтийн эсрэг бат бөх гэж нэрлэгддэг.

Bitcoin-д хамгийн урт гинжийг хамгийн их зардал гаргасан гэж үздэг PoW(Proof of Work)-ийн тусламжтайгаар зангилаа хоорондын мэдээллийг нэгэн ижил саналд нийцүүлж байгааг танилцуулсан боловч, хувийн блокчэйн оролцогч зангилааны тоог хязгаарлах боломжтой учраас, Рахос гэх мэт уламжлалт, түгээмэл тохиролцооны алгоритмыг ашиглах нь элбэг байдаг.

Нийтийн(public) болон хувийн (private) блокчэйний тохиролцооны алгоритмуудыг харьцуулбал, public блокчэйний сонгож авсан тохиролцооны алгоритм нь оролцогч зангилаануудын тоо олшрох тусам, гүйлгээний баталгаажуулалтын хурданд нөлөө гарах нь багасах шинж чанартай боловч, гүйлгээний процессын throughput/хурд/ өндөр биш юм.

Харин хувийн блокчэйн зангилаа тоо нэмэгдэхэд гүйлгээний баталгаажуулалтын



хурд буурах боловч, тогтсон тооны зангилаануудын хүрээнд өндөр throughput-тэй байж чаддаг.

### 2.4.2 Эцэслэн шийдэх чанар(finality)

Нийтийн болон хувийн блокчэйний тохиролцооны алгоритмд finalty гэж нэрлэгддэг шинж чанарын ялгаа бас бий. Finalty гэдэг нь нэг удаа хийгдсэн гүйлгээний үр дүнг цуцлахгүй(эцэслэн шийдэх) гэдгийг илэрхийлнэ. Энэ чанар нь бодит байдал дээр гүйлгээ хийх үед чухал элемент гэж хэлж болно. Оролцох зангилаа-д хязгаарлалт байхгүй нийтийн блокчэйний хувьд finalty-г авч явах нь хэцүү юм.

Жишээ нь блокчэйн дээр Батын үлдэгдэл 1000 төгрөг гэж бичигдсэн байсан гэж үзье. “Батаас Дорж уруу илгээх 600 төгрөг(шилжүүлэг БД гэе)” болон “Батаас Болд руу илгээх 700 төгрөг(шилжүүлэг ББ гэе)” нь нэгэн зэрэг өөр өөр зангилаа уруу хүсэлт(request) явсан гэж үзье

Хараахан аль ч гүйлгээ нь блокчэйн дээр тэмдэглэгдээгүй учраас хүсэлт хүлээж авсан зангилаа-ууд аль ч гүйлгээнд Батад хангалттай үлдэгдэл байгаад, гүйлгээг хийхэд асуудалгүй гэж үзнэ. 2 гүйлгээ нь 2-уулаа хүлээн зөвшөөрөгдчихвөл Батын үлдэгдэл хасах 300 төгрөг болж, систем бүхэлдээ хасах үлдэгдэл гэсэн буруу байдалд шилжчихнэ.

Энэ асуудлыг шийдэхийн тулд, [Гүйлгээ БД] юм уу[Гүйлгээ ББ]-гийн аль нь “түрүүлж үүссэн” бэ гэдгийг шийдэх шаардлага гарч байна. [Гүйлгээ БД] нь [Гүйлгээ ББ]-гээс түрүүлж үүссэн гэж үзвэл, [Гүйлгээ БД]-гийн дуусах мөчид Батын үлдэгдэл 400 төгрөг болж, [Гүйлгээ ББ] нь үлдэгдэл мөнгө хүрэлцэхгүй учраас буруу шилжүүлэг болж, блокчэйн бүртгэгдэхгүй. Эсрэгээрээ [Гүйлгээ ББ] нь [Гүйлгээ БД]-ээс түрүүлж үүссэн бол, [Гүйлгээ БД] нь буруу шилжүүлэг болно.

Нийтийн блокчэйн зангилаа бүр өөрийн хадгалж буй статус дээр үндэслэж, гүйлгээний шалгалтыг явуулдаг. Гүйлгээний шалгалт дууссан үед шалгалт дууссаныг сүлжээн доторх зангилаа-уудад цацдаг(broadcast). Шалгалт дууссан тухай мэдэгдэл хүлээж авсан зангилаа шалгалт зөв эсэхийг баталгаажуулаад өөрийн статусыг шинэчилдэг. Энэ зангилаа нь шинэ гүйлгээ шалгахгаар бол, энэхүү шинэчлэгдсэн статус дээр үндэслэж гүйлгээг шалгана.

Дээр бичсэнчлэн, өөр өөр зангилаа дээр ялгаатай гүйлгээ бүр шалгагдаж, дууссан тухай мэдэгдэл сүлжээнд цацагдсан тохиолдолд, дууссан тухай мэдэгдлийг хүлээж

авсан зангилаа өөрийн статусыг аль нэг гүйлгээний үр дүнгээр шинэчлэх шаардлага гарна. Энэ үед дууссан тухай мэдэгдэл хүлээж авсан зангилаа шалгалтын үр дүн тус бүрийн гинжний аль уртыг нь сонгож, статусаа шинэчилнэ.

Гинжний уртаас хамаарч, өмнө нь орсон гүйлгээ нь блокчэйнд бичигдэнэ. Хойно нь орсон гүйлгээний хувьд, зангилаа нь өмнө орсон гүйлгээний үр дүнг тооцсоны дараах шинэчлэгдсэн статусаар дахин шалгалт явуулна.

Дахин шалгалтын үр дүнд, гүйлгээ нь үнэн зөв байвал сүлжээн дотор дахин цацаж(broadcast) бусад зангилаа дээр хүлээж авах хүртэл хүлээнэ. Харин буруу байвал, уг гүйлгээний хүсэлт нь алдаа болно.

Өмнөх жишээн дээр, [Гүйлгээ БД]-ийн гинж [Гүйлгээ ББ]-ийн гинжнээс урт бөгөөд, [Гүйлгээ БД] нь блокчэйнд бичигдсэн гэж үзье. Үүний үр дүнд, Батын хамгийн сүүлийн үлдэгдэл 1000 төгрөгөөс 600 төгрөгөөр хасагдаж, 400 төгрөг болно. Энэ байдалд, [Гүйлгээ ББ]-г шалгаад, үлдэгдэл хүрэлцэхгүй учраас [Гүйлгээ ББ] нь буруу гүйлгээ болж алдаа болно. [Гүйлгээ БД]-г шалгасан нөхцөлийг бодож үзвэл, үлдэгдэл 1000 төгрөг байх үед шалгаад зөв гэсэн дүгнэлт хийгээд, гүйлгээг гүйцэтгэсэн(сүлжээн доторх цацсан) боловч, түүний дараагаар өөр гүйлгээ гүйцэтгэгдэж, тэр нь давуу эрхтэй байсан учраас, үлдэгдэл нь 400 төгрөг болж, [Гүйлгээ БД] нь буруу болсон байна.

Нэгэн зэрэг хийгдэх гүйлгээ нь 2-оос олонгүй байна гэж мэдэж байгаа тохиолдолд, нэг талынх нь гүйлгээг дууссаны дараа нөгөө нэгийг нь гүйцэтгэвэл, дээрх шиг цуцлах тохиолдлыг гаргахгүй байж чадна. Гэвч, тодорхойгүй олон тооны зангилаа оролцож байгаа нийтийн блокчэйнд, нэгэн зэрэг хийгдэх гүйлгээ хэд байхыг хэлж мэдэхгүй. [Гүйлгээ БД] болон [Гүйлгээ ББ]-гээс өөр гүйлгээ бас нэгэн зэрэг хийгдэж байгаад, хоёр гүйлгээ хоёулаа цуцлагдах магадлал ч бий.

Энэ мэтчилэн нийтийн блокчэйнд гүйлгээг гүйцэтгэсэн үр дүн цуцлагдахгүй гэсэн finalty гэдэг шинж чанарыг хадгалж чаддаггүй.

Харин, оролцогч зангилаа-ын тоо нь хязгаарлагдсан хувийн блокчэйнд Рахос гэх мэтийн тохиролцооны алгоритмаар гүйлгээг эцэслэж чаддаг.

Жишээ нь, бүх зангилаа-оор олонхийн саналаар [Гүйлгээ БД]-г сонгох уу эсвэл [Гүйлгээ ББ]-г сонгох уу гэдгийг шийдэж чаддаг. Сонгогдсон гүйлгээ нь гинжин дээр бүртгэгдэж, түүнээс хойш цуцлагдахгүй болно. Олонхийн саналаар шийдэж байгаа болон үр дүнг нь бүх зангилаа дээр хүргэж чадаж байгаа нь оролцогч талуудын тоог хязгаарласан учраас юм.

### 2.4.3 Ухаалаг гэрээ(Smart contract)

Bitcoin-д зоос(койн)-ны шилжилтийн мэдээллийг бүх оролцогчдод дамжуулна гэсэн тогтолцоотой байсан. Үүний дээр, өөр мөнгөний мэдээлэл болон машин, үл хөдлөх хөрөнгийн эзэмших эрх гэх мэт зүйлсийг token/кодолсон тэмдэгтийн цуваа/ болгоод bitcoin-ы гүйлгээнд нэмэлт байдлаар оруулж, эдгээрийг өгч авалцдаг болгох өнгөт койн(colored coin) гэсэн санаа бас гарч ирсэн юм. Гэсэн хэдий ч, bitcoin-ы оршин байгаа тогтолцоог тэр хэвээр нь ашиглах учраас, агуулах мэдээллийн хэмжээнд хязгаар байгаа, мөн гүйлгээнд bitcoin хэрэгтэй болох зэрэг хязгаарлалтууд байсан. Иймд, Ethereum нь ухаалаг гэрээ гэдэг ойлголтыг оруулсан блокчэйн гэдгийг гаргаж, түүний дараагаар олон тооны блокчэйн ухаалаг гэрээг оруулж ирсэн.

Ухаалаг гэрээг ашиглавал ямар зүйлийг хийж чаддаг болох вэ. Өргөн ашиглагддаг жишээ гэвэл “Автомат зарагч машинд зоос оруулахад, бараа гарч ирдэг” гэсэн дараалал бүхий урсгал бас ухаалаг гэрээ юм. Энэ мэтчилэн ямар нэг нөхцөлийн дор тогтсон үйлдэл хийдэг зүйлийг ухаалаг гэрээ гэж хэлдэг.

Ухаалаг гэрээ нь нэг үгээр хэлбэл “блокчэйн дээр ажиллана” гэсэн онцлогтой ердийн програм гэж хэлж болно. Ухаалаг гэрээ нь блокчэйн болгоноор нэршил нь өөр өөр байдаг боловч, цаанаа бодит бие нь Javascript(төрлийн хэл), Golang, Java, C# гэх мэтийн ердийн програмчлалын хэлээр бичиж болох програм бөгөөд блокчэйний статус болон хадгалагдаж байгаа дата зэргийг уншиж бичих зориулалттай зүйл юм.

Гэхдээ, “Блокчэйн дээр ажиллана” гэдэг дээр анхаарах зүйл бий. Энэ үгнээс ямар ажиллагаа төсөөлөгдөж байна вэ? Блокчэйн бүхэлдээ 1 нийтлэг процессын байгууллага, эсвэл оролцогчдын аль нэг нь төлөөлөөд програмыг ажиллуулдаг гэж төсөөлөгдөж байна уу. Үнэндээ аль алианаас нь өөр бөгөөд, бүх зангилаа дээр ижил програм ажиллаж, хариултыг нь тааруулдаг гэсэн ажиллагаа болж байгаа юм.

Блокчэйн дээр бүх зангилаа нь ижил дата хуваалцдаг, гэдгийг аль хэдийнээ тайлбарласан боловч, энэ нь ухаалаг гэрээний хувьд ч мөн нэгэн адил юм.

Ердийн програмд санамсаргүй тоо ашиглаж, гаднах өгөгдлийн эх сурвалжаас утга олж авчирч, процесс хийх зэргийг ихэвчлэн хийдэг боловч, энэ мэт тодорхой бус шинжийг агуулсан ажиллагаа нь нэгэн ижил өгөгдлийг хуваалцана гэсэн шинж чанарыг баримтлах шаардлагатай ухаалаг гэрээний хувьд чадахгүй зүйл бөгөөд детерминистик (тогтсон, тодорхой) байдлаар бүх процесс үргэлжилж байх шаардлагатай.

Ажиллуулах бүрд санамсаргүй тоо ашиглах эсвэл гадны сервертэй холбогдох шаард-

лагатай үед тэдгээр үйлдлүүдийг оgasle гэж нэрлэгддэг 3-дагч этгээдээр гүйцэтгүүлж, олсон утгыг нь ухаалаг гэрээнд дамжуулах гэсэн арга бий. Энэ тохиолдолд, блокчэйн нь зорин байж хийсэн тархмал систем учраас оgasle нь цорын ганц эвдрэлийн цэг болохооргүй байх хэрэгтэйг анхаарах хэрэгтэй.

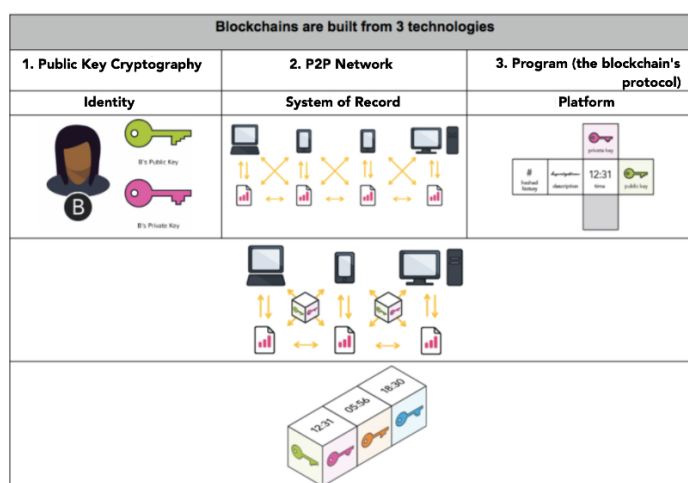
## Бүлэг 3

# Судалгаа

### 3.1 Блокчэйн технологи хэрхэн ажилладаг вэ

Онолын хэсэгт Блокчэйн технологи гэж юу болох, ямар технологиуд блокчэйнийг бүрдүүлдэг тухай бичсэн бол одоо блокчэйн технологи хэрхэн ажилладаг талаар судалснаа тайлбарлая.

Блокчэйний ажиллагаа үндсэн гурван технологид суурилдаг тухай онолын хэсэгт дэлгэрэнгүй бичсэн. Энэ гурван технологи нь 1) хувийн түлхүүрт криптограф, 2) хуваалцдаг данстай тархсан сүлжээ 3) сүлжээний гүйлгээ болон бичилт хадгалалт болон хамгаалалтын үйлчилгээ үзүүлэх технологиуд юм.

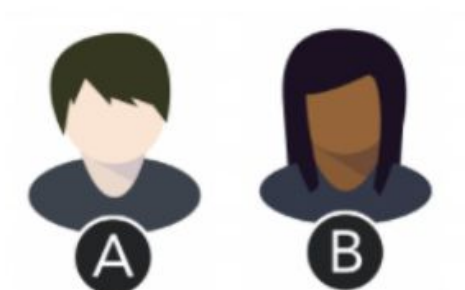


Зураг 3.1: Блокчэйний үйл ажиллагааны ерөнхий бүтэц

### 3.1. БЛОКЧЭЙН ТЕХНОЛОГИ ХЭРХЭН АЖИЛЛАДАГ ВЭҮЛЭГ 3. СУДАЛГАА

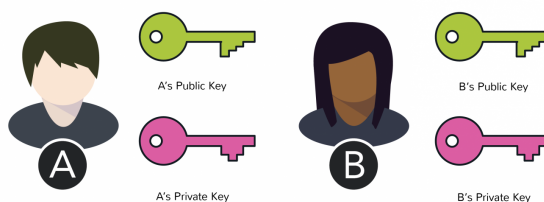
#### 3.1.1 Криптограф түлхүүр

Хоёр хэрэглэгч интернетээр гүйлгээ хийх хүсэлт гаргана :



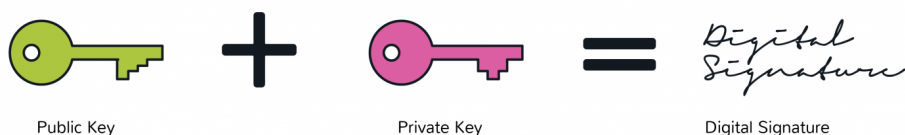
Зураг 3.2: Гүйлгээ хийх хэрэглэгчид

Хоёр хэрэглэгч тус бүр хувийн болон нийтийн түлхүүртэй.



Зураг 3.3: Хэрэглэгч тус бүр хувийн болон нийтийн түлхүүртэй

Блокчэйн технологийн энэ бүрэлдэхүүн хэсэг нь аюулгүй цахим танилт үүсгэх зорилготой. Цахим танилт нь хувийн болон нийтийн криптограф түлхүүрүүдийн хослолд суурилдаг. Тэдгээр түлхүүрүүдийн хослол нь тоон гарын үсэг болж ашиглагддаг.



Зураг 3.4: Хувийн болон нийтийн түлхүүрийн хослолоор тоон гарын үсэг үүснэ

Дан ганц найдвартай тоон гарын үсэг байлаа гээд аюулгүй цахим холбоо үүсгэ-

### 3.1. БЛОКЧЭЙН ТЕХНОЛОГИ ХЭРХЭН АЖИЛЛАДАГ ВЭҮЛЭГ 3. СУДАЛГАА

хэд хангалтгүй юм. Адилтган танилтыг шийдэхийн хажуугаар гүйлгээг батлах болон зөвшөөрөл өгөх санаа байнга хамт байх ёстой.

Блокчэйний хувьд энэ нь тархсан сүлжээгээр эхэлдэг.

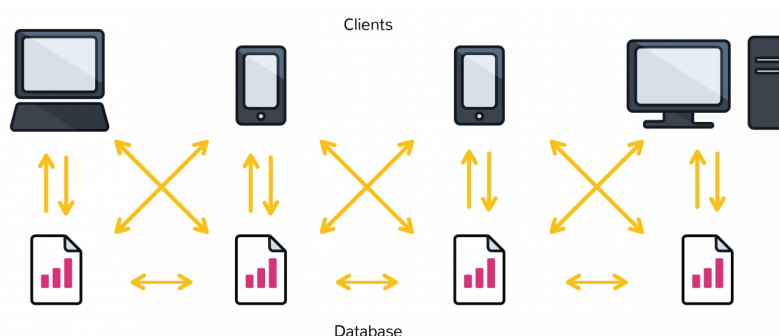
#### 3.1.2 Тархсан сүлжээ

Тархсан сүлжээ ашиглахын хэрэгцээ болон давуу талыг дараах жишээтэй харьцуулж ойлгож болно. Хэрэв ойд мод уналаа гэж үзэхэд, модыг унаж байгааг бичих камер байсан гэж үзвэл бид мод уначихсан гэдэгт эргэлзэхгүй болно. Бид юунаас болсон, хэрхэн болсон зэрэг тодорхой зүйлгүй байсан ч харсан зүйлээрээ баталгаа хийдэг.

Блокчэйний хувьд сүлжээний хэрэглэгчид нь камерын оронд математик тооцооллоор нэг зэрэг нэг зүйлийг гэрчлэх замаар баталгаажуулалтыг хийдэг. Ерөнхийдөө сүлжээ том байх хэрээр найдвартай байдал нэмэгдэнэ гэж үздэг.

Bitcoin - ний сүлжээний хамрах хүрээ нь bitcoin - ний хамгийн давуу шинж болдог. Bitcoin сүлжээнд бичилт хийх үед 3,500,000 ТН/s буюу дэлхийн томоохон 10,000 банк нийлснээс илүү хүчин чадлаар хамгаалагддаг гэсэн үг юм. Ethereum - ийн хувьд 12.5 ТН/s буюу Bitcoin - той харьцуулахад бага ч гэсэн Google - с том бөгөөд үүсээд 2 жил болж байгаа, одоогоор туршилтын шатандаа байгаа гэж хэлж болно.

#### 3.1.3 Бичилтийн систем



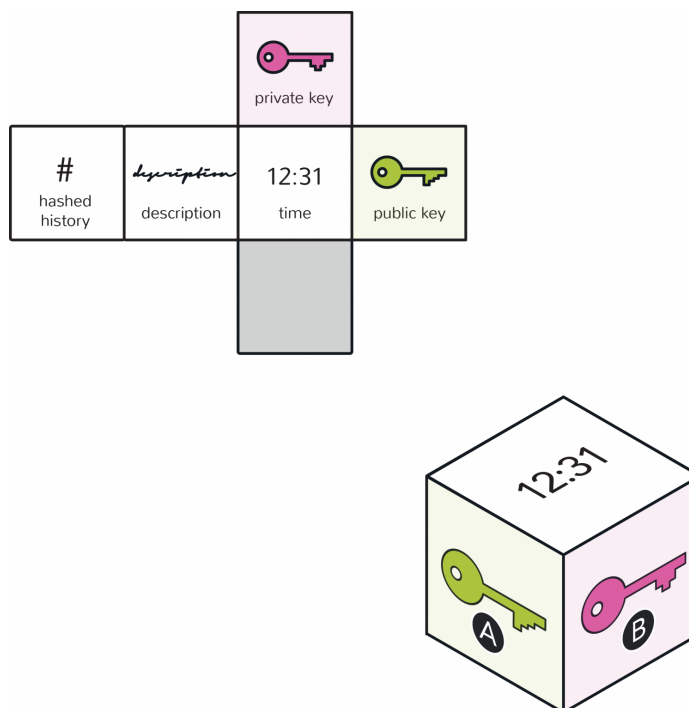
Зураг 3.5: Бичилтийн систем

Сүлжээнд криптограф түлхүүрүүд холбогдсон үед цахим харилцаанд хамгийн ашигтай хэлбэр болдог. Үйл ажиллагаа нь А хэрэглэгч өөрийн хувийн түлхүүрийг авснаар эхлэх ба зарим төрлийн мэдэгдэл үүсгэн (bitcoin - ний хувьд цахим мөнгөний нийлбэ-

### 3.1. БЛОКЧЭЙН ТЕХНОЛОГИ ХЭРХЭН АЖИЛЛАДАГ ВЭҮЛЭГ 3. СУДАЛГАА

рийг илгээх гэх мэт) В хэрэглэгчийн нийтийн түлхүүрт холбодог.

#### 3.1.4 Протокол



Зураг 3.6: Блокийн бүтэц

Блок нь тоон гарын үсэг, хугацааны тамга, холбогдох мэдээлэл зэргийг агуулах ба сүлжээн дэх бүх зангилаануудад цацагдана (broadcast).

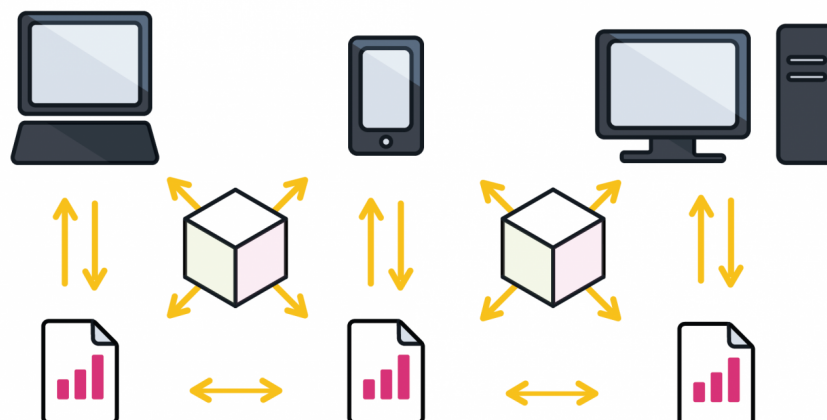
Зарим хүний хувьд "сүлжээг аюулгүй байлгахад оролцох тэр их тооцооллын чадлыг хаанаас цуглуулах юм бэ?" гэсэн асуулт гарч болно. Нээлттэй буюу нийтийн блокчэйний хувьд олборлолт (mining) гэдэг зүйл энэ асуултын хариулт болно. Компьютеруудыг сүлжээнд үйлчилснийх нь төлөө урамшуулал өгөх байдлаар блокчэйн сүлжээ ажилладаг. Хэрэглэгчийн хувийн ашиг сонирхол нийтийн хэрэгцээнд ашиглагдана гэсэн үг юм.

Bitcoin - ий хувьд протоколынх нь үндсэн зорилго нь нэг bitcoin-ийг ижил хугацаанд өөр өөр гүйлгээнд ашиглагдахгүй байлгах явдал юм. Энэ зорилгод хүрэхийн тулд сүлжээнд зангилаанууд proof-of-work математик тооцооллыг бодон bitcoin бүрд гүйлгээний түүхийг баталгаажуулж ажилладаг.

Олборлогчид ерөнхийдөө шинэ блокыг хүлээн зөвшөөрөх эсвэл хуурамч гэж үзэн

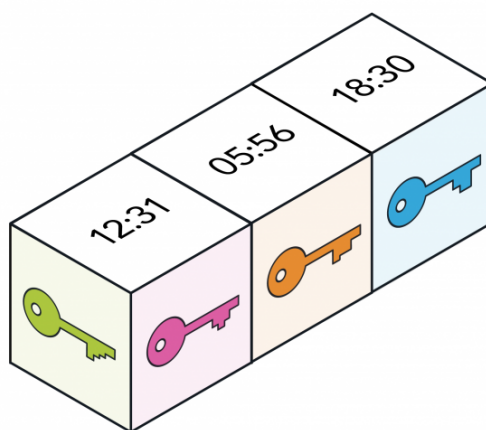


### 3.1. БЛОКЧЭЙН ТЕХНОЛОГИ ХЭРХЭН АЖИЛЛАДАГ ВЭҮҮЛЭГ 3. СУДАЛГАА



Зураг 3.7: Проткол дамжих үйл ажиллагаа

блокуг буцаах эсэхийг CPU-нийхээ хүчин чадлаар сонгон сүлжээнд саналаа өгөх үйл явцыг хийдэг. Хэрэв дийлэнх олборлогчид нэг шийдэлд санал нэгдвэл тэд тухайн блокуг гинжинд(chain) холбоно. Тухайн блок хугацаагаар тамгалагдах ба мэдээлэл болон зурвас хадгалж болно.



Зураг 3.8: Гинжинд холбогдсон блокын цуваа

Блокын төрөл, хэмжээ болон баталгаажуулалт нь блокчэйн бүрийн хувьд өөр байж болдог. Энэ нь блокчэйний протоколоос буюу ямар гүйлгээг баталгаатай гүйлгээ гэж үзэх болон үзэхгүй байх болон шинэ блокуг хэрхэн үүсгэх удирдлагын дүрмээсээ хамаардаг. Баталгаажуулалтын үйл ажиллагаа блокчэйн бүрд тусгайлан зориулагдан

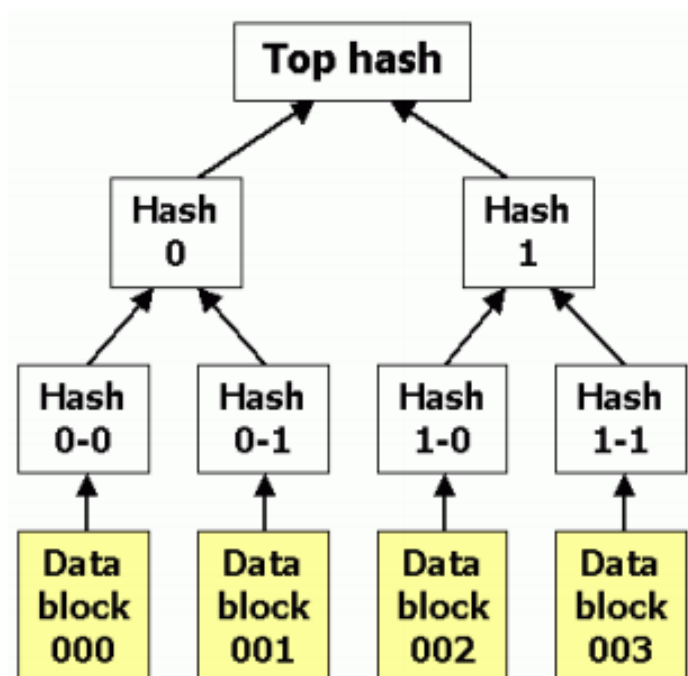
### 3.1. БЛОКЧЭЙН ТЕХНОЛОГИ ХЭРХЭН АЖИЛЛАДАГ ВЭҮЛЭГ 3. СУДАЛГАА

хийгдэж болно.

#### 3.1.5 Блок хэрхэн үүсдэг вэ

Блокчэйн технологи анхандаа Bitcoin - ий гүйлгээний нийтийн дансанд ашиглагдаж байсан. Блокчэйн тэдгээр гүйлгээг блокт хадгалж илүү олон гүйлгээ хийгдсэнээр эцэст нь блок бүрэн гүйцэд болдог. Блок бүрдмэгц утгууд linear chronological (шугаман дараалал) -р блокт нэмэгддэг.

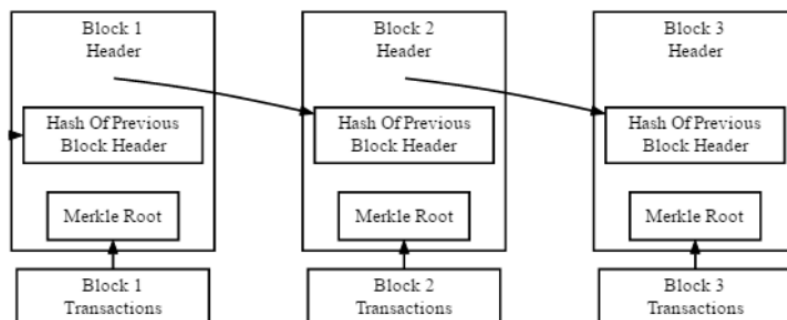
Блокчэйний анхны блокыг "Genesis block(Үүсэл блок)"өөрөөр "Block 0"гэж нэрлэдэг. Genesis блок нь ихэнхдээ програмдаа хатуугаар бичигдсэн байдаг ба өмнөх блокийн утгыг агуулдаггүйгээрээ онцлог. Genesis блок нэгэнт үүссэн бол "Блок 1"үүсэж genesis блокт залгагддаг. Блок бүр гүйлгээний мэдээллийн хэсэгтэй байдаг ба энэ хэсэгт гүйлгээ бүрийг хашлан утгыг нь хуулж аваад хос хосоор нь нийлүүлж хашладаг, энэ үйлдлийг ганц хаш үлдтэл нь давтана хийнэ(зураг 3.9). Хамгийн сүүлд үлдсэн хашийг merkle root буюу модны үндсэн гэж нэрлэдэг. Блокын толгойд (blok header) merkle root хадгалагддаг.



Зураг 3.9: Хаш хүснэгт

Гүйлгээний утгыг өөрчлөгдөөгүй гэдгийг баталгаажуулахын тулд блок бүр өмнөх

блокийнхоо толгой мэдээллийг хадгалдаг, ингэснээр мэдээллийг өөрчлөх тохиолдолд зураг 3.10 - т харуулснаар тухайн гүйлгээний утгыг хадгалж буй блокоос гадна удаах блокуудыг мөн өөрчлөх шаардлагатай болно гэсэн үг юм.



Зураг 3.10: Bitcoin блокын хялбаршуулсан загвар

Блокчэйн peer-to-peer сүлжээгээр холбогдохоор загварчлагдсан байдаг, зангилаа буюу реер бүр блок болон арилжаанд суурилан бие биетэйгээ харьцана. Нэгэнт сүлжээнд холбогдсон бол зангилаанууд сүлжээн дэх бусад зангилаануудын мэдээллийн шидэж эхэлдэг, ингэснээр тархсан сүлжээнд зангилаанууд нэг нэгнээ олох арга хэрэгждэг. Сүлжээнд зангилаа байх зорилго нь биелэгдээгүй байгаа гүйлгээ болон дөнгөж олборлосон блокийг баталгаажуулах. Зангилаа үйл ажиллагаандаа орохоос өмнө эхлээд анхны блокийг татаж авах шаардлагатай. Анхны блокийг татаж авах нь шинэ зангилааг блок 1 - с хамгийн сүүлийн блок хүртэлх бүх блокийг татуулж баталгаажуулах бөгөөд энэ үйл ажиллагаа дууссанаар тухайн зангилааг синхрончлогдлоо гэж үзнэ.

## 3.2 Блокийн багтаамж

Блокийн хэмжээ ашиглагдаж буй технологиосоо хамаарч харилцан адилгүй байна. Иймд блокчэйний хамгийн том жишээ болох Bitcoin - оор жишээ авч тайлбарлая. Bitcoin сүлжээнд хийгдэж байгаа бүх гүйлгээ энэ сүлжээнд бичигдэж байдаг, нийтийн дансуудыг дурын этгээд харж болох ч хэн ч өөрчилж чадахгүй. Тэдгээр дансууд нь блокуудаас бүрдэх ба хоорондоо криптографаар нийцэн нийлдэг.

Хэрэглэгч гүйлгээ хийх үед, гүйлгээ тухайн үед олборлогдсон блокт нэмэгдээд дараа нь тухайн блокийн удаах блокоор баталгааждаг. Гүйлгээний дээр олон блок нэмэгдэх тусам хувиршгүй байдал нь баталгаатай боллоо гэж үздэг.

Гүйлгээ нь энгийнээр тухайн гүйлгээний хураангуйлсан мэдээллийн багц бөгөөд бусад мэдээллүүдийн адил блокт нэмэгдэхдээ тодорхой зай багтаамж эзэлдэг.

Одоогийн байдлаар Bitcoin блокчэйний блок бүр 1MB хэмжээтэй мэдээллийг агуулах багтаамжтай байдаг. Энэ нь Bitcoin - ий блокт хэдэн ширхэг гүйлгээний мэдээлэл багтах нь гүйлгээний мэдээлэл өөрөө хэр хэмжээтэй гэдгээс шалтгаалж хязгаарлагдмал гэсэн үг юм. Гэвч үргэлж ийм байгаагүй.

### 3.2.1 Блок хэмжээний асуудал

Bitcoin - ий эхэн үед блокийн хэмжээ нь хязгааргүй байсан. Гэсэн ч DOS(Denial Of Service) халдлагаар их хэмжээний блок дүүргэлт үүсгэх нөхцөлөөс сэргийлж блокийн хэмжээнд анх өөрчлөлт оруулсан. Ингэснээр жирийн хэрэглэгчид Bitcoin ашиглах хугацаанд ганц л түрийвч ашигладаг байсныг өмнө нь Bitcoin QT гэж нэрлэдэг байсан бол одоо Bitcoin Core гэж нэрлэх болсон. Үүнийг хэрэглэгч блокчэйнийг бүхлээр нь татаж авахад шаардагддаг бөгөөд энэ нь хэрэв хэрэглэгч томоохон хэмжээний блок үүсгэх бол, тухайн түрийвч ажиллаж байгаа энгийн компьютер хэзээ ч гүйцэхгүй бөгөөд энэ шалтгаанаар зарим хэрэглэгчид хэзээ ч bitcoin - оо зарцуулах боломжгүй болно гэсэн үг юм.

Өнөө үед маш олон хүн блокийн хэмжээг хязгаарлах нь одоо цагт ямар ч хэрэггүй ба ингэж хязгаарлах нь тухайн цахим мөнгийг нийтийн хэрэгцээнд хангалттай хүргэж тэлэх боломжгүй болгож Bitcoin - ийг зарим талаар гэмтээж байгаа гэж үздэг. Одоогийн байдлаар Bitcoin секундэд 4-7 н гүйлгээг хийх боломжтой байгаа, энэ нь VISA болон PayPal зэрэг системтэй харьцуулахад тааруу үзүүлэлт юм.

Энэ асуудал Bitcoin хэрэглэгчдийн дунд багтаамжийн хязгаарлалтыг дэмжих болон үгүйсгэх байдлаар маш том маргааныг үүсгэсээр байна. Ихэнх нь блокийн багтаамжийг ихэсгэснээр Bitcoin олборлолтын төвлөрөлд нөлөөлж багтаамж ихсэхийн хэрээр олборлох төхөөрөмжийн шаардагдах хүчин чадал өснө гэж үзэж байгаа бол үлдсэн хэсэг нь багтаамжийг ихэсгэх нь Bitcoin - ийг бусад өргөн хэрэглээний төлбөрийн системүүдтэй өрсөлдөхүйц хэмжээнд хүргэнээ гэдэг талаас нь харж байна.

Эцэст нь зөвхөн олборлогчид болон бүр зангилаа хэрэглэгчид л coin - ийг үүсгэж гүйлгээг баталгаажуулж байгаа тул тэдэнд шийдвэр гаргах эрхтэй байдаг. Гэвч тэд дэлхийгээр тархсан, төвлөрсөн бус, мөн тэд ихэвчлэн хэн гэдэг нь ч мэдэгдэхгүй нууцлагдмал байдаг. Харин сүлжээний хэсэгт салаалалт үүсгэх болбол дийлэнх олборлогчид

болон бүрэн зангилаанууд өөрчлөлтийг хүлээн зөвшөөрсөн байх ёстой.

### 3.2.2 Давуу тал

Блокийн хэмжээ их байх маш олон шалтгаанууд байдаг. Одоогийн блокийн хэмжээ Bitcoin - ийг зөвхөн 4-7 гүйлгээг нэг секундэд хийх хязгаартай болгодог. Ингэснээр жирийн хэрэглэгчдийн дунд яаралтай гүйлгээ хийх өрсөлдөөнөөс шалтгаалж гүйлгээний зардал өсөж яваандаа Bitcoin хангалттай алдартай болох үед зарим хэрэглэгчид сүлжээнээс шахагдан гарах нөхцөл үүснэ.

Блокийн хэмжээ ихэссэнээр хэрэглэгчид өндөр төлбөр төлөлгүйгээр олборлогчид илүү ашиг хүртэх боломжтой болно.

Түүнчлэн олон хүн блокийн хэмжээг ихсэх нь зангилаануудад маш их ачаалал нэмж, хадгалах төхөөрөмжийн багтаамж өндөр байхыг шаардана гэдгийг сануулж байгаа юм. Иймд блокийн хэмжээг нэг шөнийн дотор л экспоненциалиар өсгөхгүй ба, сүлжээнд хэрэгцээ гарахтай зэрэгцэн бага багаар ихэсгэх хэрэгтэй гэж үзэж байгаа.

### 3.2.3 Сул тал

Хэдий блокийн хэмжээ том байх хэрэгтэй гэдэгт олон хүн санал нэгтэй байгаа ч блокийн хэмжээг 1MB -д хязгаарлах нь зүйтэй гэж үзэх хуучинсаг үзэлтэй талд мөн л хангалттай үндэслэлтэй шалтгаан байгаа юм.

Бүрэн зангилаа хэрэглэгчдийн дунд зурвасын өргөний шаардлага байх бөгөөд энэ нь нэмэгдсээр бүрэн зангилааны тоо цөөрөх талтай.

Түүнчлэн сүлжээний хамрах хүрээг өсгөхөд заавал том хэмжээтэй блок, эсвэл хатуу салаалалтын шаардлагагүй segwit, sidechain гэх зэрэг шийдлүүд байдаг тул блокийн хэмжээг ихэсгэх нь чухал биш гэж үзэх хүн олон байдаг.

Мөн Bitcoin - ийг хатуу салаалалтаар өөрчлөх нь тогтворгүй байдал үүсгэх бөгөөд ингэж сүлжээг хувааснаар салаалсан хоёр блокчэйн бэрхшээлтэй учрах зам болно гэж үздэг.

## Бүлэг 4

### Төслийн хэсэг